3-2003

# Performance Evaluation and Analysis of Effective Range and Data Throughput for Unmodified Bluetooth Communication Devices

Timothy F. Kneeland


# Performance Evaluation and Analysis of Effective Range and Data Throughput for Unmodified Bluetooth Communication Devices

THESIS

Timothy F. Kneeland, Captain, USAF
AFIT/GCS/ENG/03-08

**DEPARTMENT OF THE AIR FORCE**

**AIR UNIVERSITY**

## AIR FORCE INSTITUTE OF TECHNOLOGY

**Wright-Patterson Air Force Base, Ohio**

AFIT/GCS/ENG/03-08

# Performance Evaluation and Analysis of Effective Range and Data Throughput for Unmodified Bluetooth Communication Devices

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Computer Science

Timothy F. Kneeland, BS, MS

Captain, USAF

March 2003

AFIT/GCS/ENG/03-08

# Performance Evaluation and Analysis of Effective Range and Data Throughput for Unmodified Bluetooth Communication Devices

Timothy F. Kneeland, BS, MS

Captain, USAF

Approved:

| | |
|---|---|
| Richard A. Raines | 10 Mar 03 |
| Dr. Richard A. Raines<br>Thesis Advisor | Date |
| Rusty O. Baldwin | 10 Mar 03 |
| Major Rusty O. Baldwin, Ph.D.<br>Committee Member | Date |
| Michael A. Temple | 10 Mar 03 |
| Dr. Michael A. Temple<br>Committee Member | Date |

**Acknowledgements**

Thank you to my wife and family for their continual support during our time at AFIT and especially during the period of this research. Angie has continually believed in me even when she did not share my views or even understand what I was talking about. For this I am thankful.

Thank you to my thesis advisor, Dr. Richard Raines, whose guidance and instruction has been a motivation for this work. Also, I'd like to extend appreciation to my committee members, Maj Rusty Baldwin and Dr. Michael Temple, who took the time to answer my questions on those areas outside my knowledge base. Maj Baldwin's instruction on data analysis and Dr. Temple's explanation of antenna properties greatly helped me achieve the goals of this study.

Timothy F. Kneeland

## *Table of Contents*

## *List of Figures*

## *List of Tables*

***Abstract***

The DoD and the Air Force continually seek to incorporate new technology in an effort to improve communication, work effectiveness, and efficiency. Office devices utilizing Bluetooth technology simplify device configuration and communication. They provide a means to communicate wirelessly over short distances thereby eliminating the need for different vendor specific cables and interfaces. One of the key concerns involved in incorporating new communication technology is security; the fundamental security concern of wireless communication is interception. Studies focusing on IEEE 802.11b have shown vulnerability zones around many DoD installations that reflect the ranges at which wireless communications using the 802.11b standard can be intercepted.

This research identifies the vulnerability zones in which Bluetooth transmissions can potentially be intercepted. Specifically, the orientation of Bluetooth device antenna and the distance between devices are varied to determine ranges at which set levels of throughput can be achieved for a specific device configuration. Throughput ranges are then mapped to graphically reflect vulnerability zones. This research shows that the range at which Bluetooth communication can occur with unmodified devices is more than twice that of the minimum standard of 10 m outlined in the core specification without degradation of the best-case throughput level measured. It is expected that the throughput ranges could be greatly extended with some device modification. This research shows that the security risk associated with interception of Bluetooth communications is legitimate and warrants further study.

# Performance Evaluation and Analysis of Effective Range and Data Throughput for Unmodified Bluetooth Communication Devices

## *1. Introduction*

### 1.1 Introduction

The ability of the Department of Defense (DoD) and the Air Force to accomplish their missions relies heavily on the ability to communicate. Rapid communication of information is the grease that turns the wheels of daily operations. The continual rapid development of new technology provides smaller, faster, and cheaper means of communication. Both the DoD and the Air Force continually seek to incorporate new technology in an effort to improve communication, mission effectiveness, and efficiency.

Office devices utilizing Bluetooth technology simplify device configuration and communication. They provide a means to wirelessly communicate over short distances thereby eliminating the need for different vendor specific cables and interfaces. Bluetooth provides a standard interface that all equipped devices can access and communicate through.

Incorporation of new technology into any existing operation does not come without a price. One of the key concerns involved in communication is security; the fundamental security concern of wireless communication is interception. There are many ways of increasing the difficulty of interception such as implementation of spread spectrum techniques or encryption. However, even with these measures it is possible for communications to be intercepted.

## 1.2 Background

The Air Force Information Warfare Center (AFIWC) continually studies different protocols and communication standards in use today in an effort to improve the level of security. Studies focusing on IEEE 802.11b have shown vulnerability zones around many DoD installations. These zones reflect the ranges at which wireless communications using the 802.11b standard can be intercepted. With the advent of Bluetooth technology and its pending incorporation into the workplace, it is important that the same concerns with 802.11b also be addressed for Bluetooth. Specifically, the need exists to determine Bluetooth transmission interception vulnerability regions.

Although these vulnerability zones are not easily exploited, they are cause for concern. They are an inherent weakness of wireless communications that is often exploited. When a weakness cannot be eliminated, it must be managed to minimize the possible effects of its exploitation.

The simplest way to manage the security weaknesses of the Bluetooth protocol is to minimize the possibility of packet transmission interception. This could be accomplished by limiting the physical radius of transmission to within the boundaries of a controlled area. If transmissions are not receivable outside the controlled area, and the personnel and equipment within the controlled area are trusted, then the possibility of packet transmission interception is minimized. Thus, the need to establish transmission reception ranges of Bluetooth devices is clear.

## 1.3 Research Focus

The primary focus of this research is to provide a basic measurement of the transmission range of commercially available Bluetooth devices. This range

measurement provides an initial look at the capabilities of the Bluetooth standard in regards to throughput over different distances. By providing the ranges at which different levels of throughput are possible, this study helps to define the proximity distance needed to intercept Bluetooth transmissions.

### 1.3.1 Objectives

This research has two objectives. The first objective is to identify the best antenna orientation for a common use configuration of Bluetooth devices. Each network device (laptop) is configured with a Bluetooth transmitter utilizing a small micro-strip patch antenna. The relative transmitter/receiver antenna orientation is expected to be significant in determining ranges of throughput.

The second objective is to utilize the antenna orientation identified by the first objective to determine ranges at which fixed levels of throughput can be received. The throughput levels for this study are 300 kbps, 200 kbps, and 100 kbps. The ranges at which these levels of throughput can be received for a set receiver orientation are identified and mapped.

The two objectives above outline this research. Identification of the best antenna orientation is important in properly identifying the throughput ranges. The primary objective is the identification of ranges at which a certain threshold of throughput can be achieved. This supports the primary focus of this research in identifying vulnerability ranges of commercially available Bluetooth devices.

### 1.3.2 Approach

This study follows a process to accomplish the above objectives. First, a review of published literature on the Bluetooth standard as well as the Bluetooth core

specification is conducted. Next, a study of a wireless sniffing application for 802.11b (Kismet) is done to determine if the same functionality could be incorporated into an application for Bluetooth. Then, an experiment to meet the first objective is conducted utilizing the Bluetooth Receiver Signal Strength Indicator (RSSI) as a metric.

The RSSI is used since it is the only signal power function provided in the Bluetooth specification. The RSSI values are captured for different orientations and distances and the data is analyzed to determine statistical significance. Findings relevant to the throughput range experiment are incorporated. Next, the throughput range experiment is developed and data measurements are taken. This data is sampled using best-case results – multiple samples are taken, but only the best is recorded. Last, a map of the throughput ranges is constructed reflecting the distances at which fixed levels of throughput were received.

## 1.4 Summary

The primary focus of this research is to provide a basic measurement of the transmission range of commercially available Bluetooth devices. A methodology is defined for identifying orientation and throughput ranges by varying antenna orientation and device distance to meet the objectives. This research is restricted to specific hardware in a particular environment. It provides a foundation for further study of Bluetooth transmissions.

The rest of this document is presented as follows. Chapter 2 provides an overview of wireless communication technologies and detailed information on the Bluetooth standard. Next, wireless security is discussed followed by Bluetooth specific security concerns. Chapter 3 outlines a detailed methodology for accomplishing the

objectives of this research. Chapter 4 discusses the experiments conducted, the data gathered, and analysis of the resulting data. In Chapter 5, a summary of the research and conclusions are presented.

# *2. Background*

## 2.1 Introduction

This chapter includes background information helpful in establishing the foundation for the research. The areas covered are wireless communications, Bluetooth, wireless communication security issues, and Bluetooth specific security issues. A brief discussion of each of these areas is presented.

## 2.2 Wireless Communications

Wireless communication encompasses transmitting signals through air and space using radio frequencies of the electromagnetic spectrum. Both international organizations and national governments govern frequency allocation. In the United States, the Federal Communication Commission regulates all commercial frequencies and their allocation. The data carrying capacity and bandwidth of a wireless system is dependent on where in the spectrum the transmission frequency is located. The higher the frequency the larger its capacity for transmitted information, but the more susceptible the transmission becomes to interference due to atmospheric conditions. Additionally, signal transmission becomes "more directional (line of sight)"[12].

Local area networks (LANs) using wireless technologies are becoming more and more common. Utilizing wireless technology facilitates LAN implementation inside and between buildings. Additionally, wireless technologies are used to "provide high-speed access to the Internet or to build metropolitan area networks"[12]. The latest addition is the advent of mobile computing using higher data rates. These higher data rates facilitate operation comparable to "traditional wired networks".

A family of protocol specifications developed by the Institute of Electrical and Electronics Engineers (IEEE) governs wireless local area networks (WLANs). The 802.11 family consists of four specifications: 802.11, 802.11a, 802.11b, 802.11e, and 802.11g. "All [five] use the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance) for path sharing."[10]. An additional new family of protocol specifications is currently in development by an IEEE working group and a special interest group. The 802.15 family (a.k.a. Bluetooth) consists of 802.15.1, 802.15.3, and 802.15.4. This protocol family will be described below.

### 2.2.2 Protocols

802.11 was the first standard in the 802.11 family. It was accepted by the IEEE in 1997 and uses phase shift keying modulation to transmit in the 2.4 to 2.48 GHz range. It provides a data rate of 1 to 2 Mbps using either Frequency Hopping Spread Spectrum (FHSS) or Direct Sequence Spread Spectrum (DSSS).

#### 802.11a

"The 802.11a specification applies to wireless ATM systems and is used in access hubs. The 802.11a protocol operates at radio frequencies between 5 GHz and 6 GHz. It uses a modulation scheme known as orthogonal frequency-division multiplexing (OFDM) that makes possible data speeds as high as 54 Mbps, but most commonly, communications take place at 6 Mbps, 12 Mbps, or 24 Mbps"[10].

#### 802.11b

Commonly referred to as Wi-Fi, 802.11b is backward compatible with 802.11. It uses complementary code keying (CCK) and transmits at 11 Mbps in the 2.4 GHz range. It is less susceptible to multipath-propagation interference than 802.11.

**802.11e**

802.11e focuses on increasing the bandwidth efficiency of 802.11a and to incorporate Quality of Service (QoS) to both 802.11a and 802.11b. It strives to increase the sustainable throughput of 802.11a to around 35 Mbps. It has the capability to manage bandwidth by assigning some packets a priority and by controlling the number of media streams on the network.

**802.11g**

802.11g is the most recently approved standard and offers relatively short range wireless transmission at rates up to 54 Mbps. "Like 802.11b, 802.11g operates in the 2.4 GHz range and is thus compatible with it"[10].

**802.15.1**

Commonly known as Bluetooth, 802.15.1 is the primary protocol standard in the 802.15 family. It operates in the 2.45 GHz band and transmits at a rate of up to 1 Mbps.

**802.15.3**

802.15.3 transmits in the 2.45 GHz band as well and "focuses on high-bandwidth (about 55 Mbps), low-power MAC and physical layers"[13].

**802.15.4**

802.15.4 also works in the 2.45 GHz band, but differs from 802.15.3 in that it "deals with low-bandwidth (about 250 Kbps), extra-low power MAC and physical layers"[13].

### 2.2.3 Transmission Methods

There are many different ways that wireless communications can occur. Each method provides certain advantages that tend to compensate for the disadvantages of

other methods. Common among these methods are narrow band, spread spectrum, and frequency hopping spread spectrum.

#### 2.2.3.1 Narrow Band

Narrow band transmissions occur within a specific frequency interval. "The signal occupies a narrow band that is susceptible to interference, either accidental or malicious"[12]. These transmissions can be intercepted easily with a radio receiver tuned in to the appropriate frequency.

#### 2.2.3.2 Spread Spectrum

Spread spectrum transmissions spread the signals out over a very wide frequency interval using one of two techniques: Direct Sequence Spread Spectrum or Frequency Hopping Spread Spectrum.

##### 2.2.3.2.1 Direct Sequence Spread Spectrum

In direct sequence, multiple bits called "chips" are used to represent each bit of data to be transmitted. If 200 chips represent each bit, then the signal is spread out 200 times its original size. The signal power is transmitted in noisy bands at power levels below the noise, thus it does not interfere with other signals in that band. In order to spread out the data stream, the sender generates a pseudorandom bit stream that modulates the original data stream. The receiver, using the same pseudorandom bit stream, then demodulates the transmitted stream.

##### 2.2.3.2.2 Frequency Hopping Spread Spectrum

Frequency hopping spread spectrum differs from direct sequence in that "the original data signal is not spread out, but is instead transmitted over a wide range of frequencies that change at split second intervals"[12]. In order to do this, a "hopping"

table is established that both the transmitter and receiver follow. They both jump from frequency to frequency in synchronization so that a jammer or interceptor would have a difficult time targeting a specific frequency.

## 2.3 Bluetooth

In late winter of 1998, five companies, Ericsson, IBM, Intel, Nokia, and Toshiba, jointly formed the Bluetooth Special Interest Group (SIG). The purpose of the Bluetooth SIG was "to develop and promote a global solution for short-range wireless communication operating in the unlicensed 2.4 GHz ISM (industrial, scientific, medical) band"[4]. The SIG elected to share all of the intellectual property of the new specification royalty-free in order to entice new members to join the SIG and adopt the technology into new products being introduced to the market.

The selection of the name Bluetooth for the new standard "comes from the Danish king *Harald Blåtand* (Bluetooth)"[2] of the 10th century and who is believed to have united the Scandinavian people. In the same way, Bluetooth aims to unite personal computing devices.

By May of 1998 there were approximately 70 adopter members in the Bluetooth SIG. The Bluetooth specification version 1.0A became publicly available in the summer of 1999 and is composed of two parts: "the core specification defining the radio characteristics and the communication protocols for exchanging data between devices over Bluetooth links"[2], and "the profile specification that defines how the Bluetooth protocols are to be used to realize a number of selected applications"[2]. Four additional members, 3Com, Lucent, Microsoft, and Motorola, joined the promoter group in

December of 1999 bringing the membership total to nine. As of January 2002 there are over 2000 adopter members of the Bluetooth SIG.

Bluetooth wireless technology is primarily aimed at replacing the interconnecting cables between many different personal devices. These devices include cellular phones, personal digital assistants (PDAs), laptop computers, and digital cameras. Many personal devices currently use proprietary connectors making it difficult to interconnect devices from different manufacturers. Thus, Bluetooth is designed to be a flexible connector facilitating the connection of several different personal devices.

Devices employing Bluetooth will "operate in the unlicensed ISM band at 2.4 GHz and employ frequency-hopping (FH) spread spectrum technology to reduce interference and fading"[14]. Full-duplex transmission is accomplished using a Time-Division Duplex (TDD) scheme and is capable of both data and voice transmissions. Up to eight different devices are able to connect to each other to form a Wireless Personal Area Network (WPAN) referred to as a piconet. One of the devices takes on the role of the "master" and the other seven are "slaves". Bluetooth WPANs are able to support asynchronous data links with each device in the WPAN and up to three synchronous voice links between the master and the slaves. A WPAN range is 10 m with transmitter power at 1 mw. This range is extendable up to 100 m by increasing the transmitter power to 100 mw.

The ISM band in most countries includes the frequency range from 2400 to 2483.5 MHz. Bluetooth utilizes the RF channels from 2402 to 2480 MHz. Table 1 shows the frequency assignments currently in place.

Each channel has a spacing of 1 MHz resulting in 79 channels for transmission. The "Bluetooth radio hops from channel to channel at 1600 hops per second"[14], thus it moves from channel to channel every 625 msec. The hopping sequence for each piconet is unique and is "determined using an algorithm based on the address (and clock) of the Bluetooth hub (master)"[14]. In order for a device to transmit in a particular piconet, it must first synchronize to this hopping sequence.

**Table 1. Bluetooth International Frequency Bands [1]**

| Area | Frequency Band (GHz) | Bluetooth Channels |
|---|---|---|
| USA, Europe and most other countries | 2.400 – 2.4835 | 79 |
| Spain | 2.445 – 2.475 | 23 |
| France | 2.4465 – 2.4835 | 23 |

A binary system of Gaussian Frequency Shift Keying (GFSK) is used for modulation by Bluetooth radios. The main reason for using GFSK is its spectral efficiency over Frequency Shift Keying (FSK). A Gaussian filter is placed in line with the FSK modulator to smooth out and shape the pulse thus narrowing the spectral width and limiting the out of band spectrum. A logic "1" is represented by a positive frequency deviation and a "0" is represented by a negative frequency deviation. Bluetooth supports a data transmission rate of 1 Mb/second. Table 2 provides a comparison between IEEE 802.11 and the Bluetooth specifications.

The Bluetooth protocol stack consists of two categories: the *transport* and the *middleware* protocols. This grouping suggested by [2] and is not part of the Bluetooth specification. "The transport protocols comprise protocols developed exclusively for the Bluetooth wireless technology". All data communication between two Bluetooth devices involves the transport protocols. Other adopter protocols and some Bluetooth specific

protocols comprise the middleware protocols. These shield different applications, "legacy and new", from the specifics of the Bluetooth transport protocols and allow them to exchange data utilizing Bluetooth wireless technology. Although different applications "may run over different protocol stacks"[11], each of these protocols accesses the Bluetooth data link and physical layer. Figure 1 shows a representation of the Bluetooth protocol stack.

**Table 2. 802.11b vs. Bluetooth [14]**

| Comparison of IEEE 802.11 / 802.11b and Bluetooth Specifications | | |
|---|---|---|
| Specification | IEEE 802.11 / 802.11b Wireless LAN | Bluetooth |
| Applications/Market | – Home<br>– School<br>– Enterprise<br>– Ad Hoc networking<br>– Campus-wide voice and data | – Cable replacement<br>– Ad Hoc networking<br>– Personal area voice and LAN access |
| Technology | – 2.4 GHz ISM<br>– Direct Sequence Spread Spectrum<br>– Frequency Hopping Spread Spectrum<br>– Infrared (IR) | – 2.4 GHz ISM<br>– Frequency Hopping Spread Spectrum; 1600 hops per second |
| Data Rate | – Direct Sequence: 11 Mbps<br>– Frequency Hopping: 1.2 Mbps | – 1 Mbps |
| Power | 20 dBm (typical) | 0 dBm, 20 dBm |
| Range | 100 m | 1-10 m at 0 dBm; 100 m at 20 dBm |
| Networking Topology | Vendor dependent access points with client adapters; each access point supporting typically 128 devices | 8 devices in a Piconet |
| Separate Voice Channel | Optional | Yes |
| Security | Optional Wireless Equivalent Protection (WEP) | Encryption, authentication |

The focus of the design of the Bluetooth protocols and the protocol stack is to maximize the re-use of existing protocols. This helps ensure smooth interoperation and

interoperability of existing (legacy) applications. Using this, "many applications already developed by vendors can take immediate advantage of hardware and software systems, which are compliant to the (Bluetooth) Specification"[11].

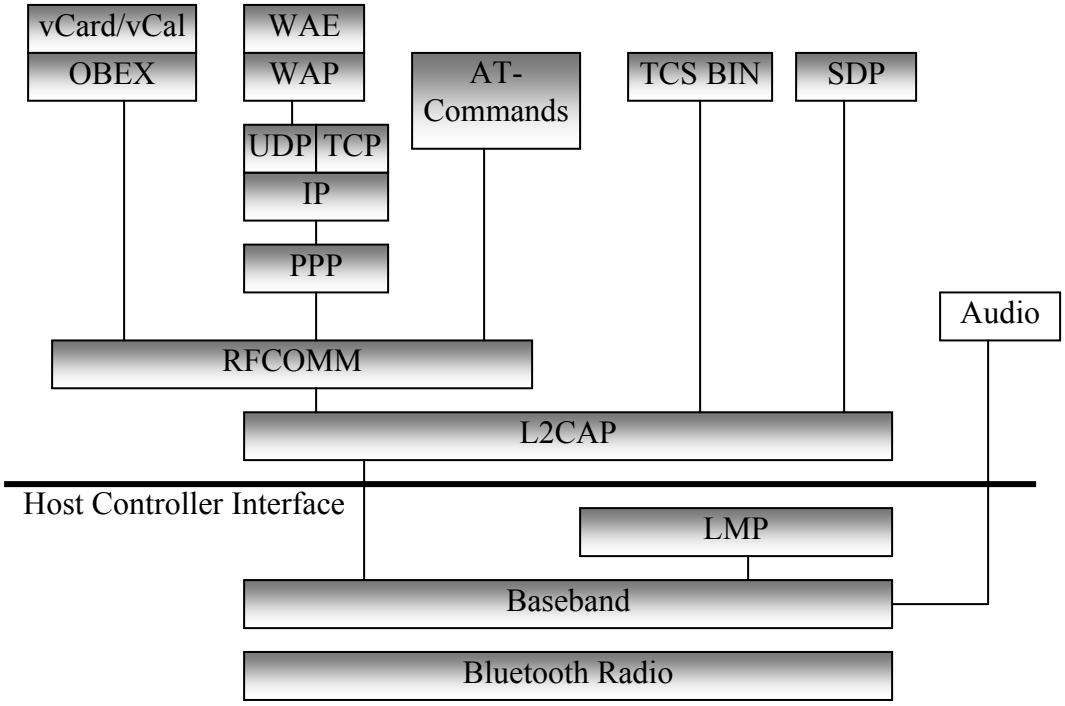


**Figure 1. Bluetooth Protocol Stack [11]**

### 2.3.1 Transport Protocol Layers

#### 2.3.1.1 Radio Layer

The radio layer has already been addressed in the above paragraphs.

#### 2.3.1.2 Baseband Layer

The baseband layer defines the physical RF link and how piconets are formed. The sharing of transmission resources among the devices of a piconet and low-level packet types are also defined by the baseband layer. Both inquiry and paging procedures are used "to synchronize the transmission hopping frequency"[11] between devices in the piconet as well as their individual clocks.

Two parameters are required for Bluetooth devices to talk to each other: the *Bluetooth device address (BD_ADDR)* and the clock. Each Bluetooth device has a unique IEEE-type 48-bit address assigned during manufacturing. The address "is engraved on the Bluetooth hardware and it cannot be modified"[2]. The clock is a free running 28-bit counter. It increments once every 312.5 microseconds, "which corresponds to half the residence time in a frequency when the radio hops at the nominal rate of 1,600 hops/sec"[2]. Once a Bluetooth device acquires these two parameters from another, they are able to communicate.

Piconets are formed ad hoc without any infrastructure assistance. The duration of a piconets existence is governed only by how long its master requires it and is able to communicate with other devices in the piconet. Bluetooth devices in a piconet take on either the role of *master* or *slave*. Only one master and up to seven slaves can exist relative to a particular piconet. The slaves are defined by whom the master is actively communicating with. More Bluetooth devices can be in a particular piconet, but only eight (one master and seven slaves) can be active at a given time. Any "Bluetooth radio may serve either as master or slave at different times"[2]. When a new device joins a preexisting piconet it is initially a slave, but immediately upon joining the new device can negotiate to become the master.

Each actively participating slave in a piconet is identified by a locally unique *active member address (AM_ADDR)* assigned by the master. The master regulates and controls transmissions in the piconet. Those devices in the piconet that are not active are considered *parked*. If a device is not part of any piconet it is considered in *stand-by* mode. Two or more piconets "can coexist in time and space independent of each

other"[2]. A Bluetooth device can join more than one piconet forming a *scatternet*. Figure 2 depicts a possible piconet and scatternet configuration.

Members of a piconet communicate by following a sequence of frequency hops in a synchronized manner. Each transmit and receive time slot lasts 625 microseconds, the duration of one nominal frequency hop. A transmission must begin and complete within a given slot. The exception to this is when a packet occupies three or five slots. To accommodate these multi-slot packets, hopping is suspended during transmission. Upon completion of transmission, the hop frequency catches up to the frequency it would have been had only single-slot transmissions occurred.

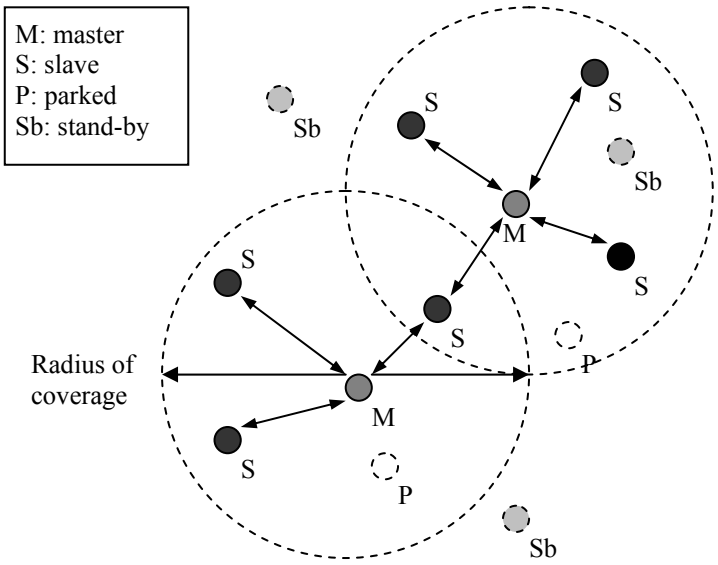


**Figure 2. Piconets and Scatternets [2]**

A slave can recreate the frequency hop sequence for a piconet by utilizing the Bluetooth address of the master device. The master's clock identifies the slot transmission frequency. Thus for scatternets, a Bluetooth device can only be master in one piconet of the scatternet since it is the sole identifier of the communications channel for its piconet.

The master's Bluetooth clock governs the synchronization of the slaves. Each slave maintains "the offset time between their own Bluetooth clock and that of their

master"[2]. The value of the second least significant bit of the master's Bluetooth clock identifies each transmission slot as either even or odd, since the clock ticks twice every 625 microseconds.

A *time-division duplex* (TDD) scheme is used to alternate between the master and the slave transmissions. "The master transmits on the even numbered slots, as defined by the master's Bluetooth clock, while the slaves transmit on odd numbered slots"[2]. A slave cannot transmit until it has received a transmission from the master. Upon receiving the master's transmission, the slave is free to transmit in the next time slot. Bluetooth devices are limited to transmitting and/or receiving in only one piconet at a time due to the different frequency hopping sequences, but a device may use non-overlapping time intervals to time-share its participation in two or more piconets.

In order for a device to acquire the *BD_ADDR* and clock of the master, two processes must occur: *inquiry* and *paging*. "The inquiry process is a device discovery process during which the master of a future piconet discovers other devices in its vicinity"[2]. The master transmits inquiry messages to inform all devices in range of its presence. Other Bluetooth devices in *discovery mode* perform an inquiry scan to search for inquiry messages and respond with a message containing their *BD_ADDR*.

The master device now enters the paging process whereby it pages particular devices to join its piconet. If the master is already aware of devices in its vicinity, it may skip the inquiry phase and simply page the device directly. The receiver of the page may now join the piconet.

Bluetooth supports two different links for transmission of packets: *asynchronous connectionless* (ACL) and *synchronous connection-oriented* (SCO). ACL is best used for

asynchronous data traffic that requires a certain level of integrity. This is accomplished through the use of retransmissions, sequence members, and forward error correction codes (FEC) if needed. SCO is primarily for audio transmissions. It transmits at 64 Kb/s in both directions for up to three links. FEC may be used by SCO traffic to correct errors, but no SCO traffic is retransmitted.

There are five different types of baseband packets as shown in Figure 3:

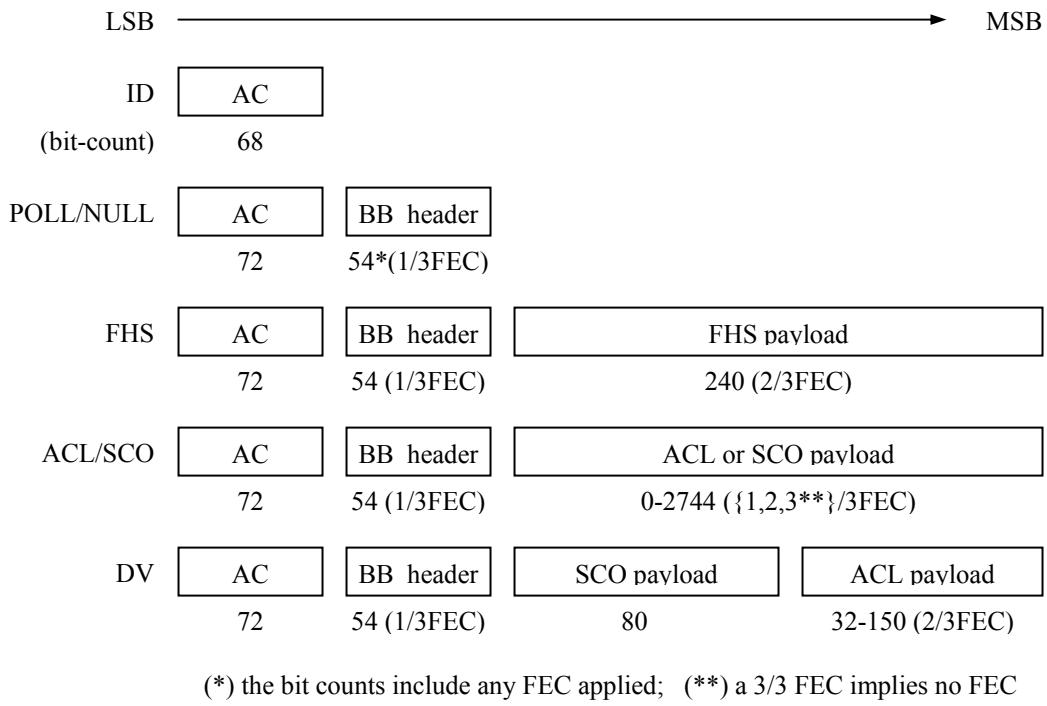


**Figure 3. Baseband Packet Types [2]**

Identification (ID), POLL/NULL, Frequency-Hopping Sequence (FHS), ACL/SCO, and Data Voice (DV). Each of these packet types contains "an *access code* (AC) field, which is used to distinguish transmissions in different piconets" [2]. Additionally, all have a header field except for the ID packet. FHA, ACL/SCO, and DV also have a payload section. Table 3 compares baseband packet types.

**Table 3. Baseband Packet Comparison**

| Packet Type | Purpose |
|---|---|
| ID | Inquiry searches; synchronization during pages |
| POLL | Explicitly poll a slave; no payload |
| NULL | Acknowledge a transmission; no payload |
| FHS | Creation of a piconet; passing address (*BD_ADDR* and *AM_ADDR*) and clock information; payload encoded using shortened Hamming code with rate 2/3 |
| ACL | Asynchronous data; payload may be encoded using FEC with rate 2/3 or not at all |
| SCO | Synchronous data; payload may be encoded using FEC with rate 1/3 or 2/3 |
| DV | Contains both ACL and SCO data; transmitted as an SCO packet; used when ACL data need to be sent to the receiver of an SCO transmission |

Each packet consists of multiple fields as depicted in Figure 4. The header contains the *AM_ADDR*, *PDU_type*, flags, and a header error check (HEC) code. "The *AM_ADDR* field identifies the destination slave of a master transmission or the source slave of a slave transmission" [2]. Bluetooth supports broadcasting of packets to all the slaves from the master by setting the *AM_ADDR* = b'000'. The slaves are not required to acknowledge receipt and no broadcast message is repeated. The PDU_type field identifies packet type. Transmission and retransmission of ACL packets is controlled by the flags using "a stop-and-go ARQ scheme and a 1-bit sequence number" [4] and flow control. The HEC provides an 8-bit code for protecting the header from errors.

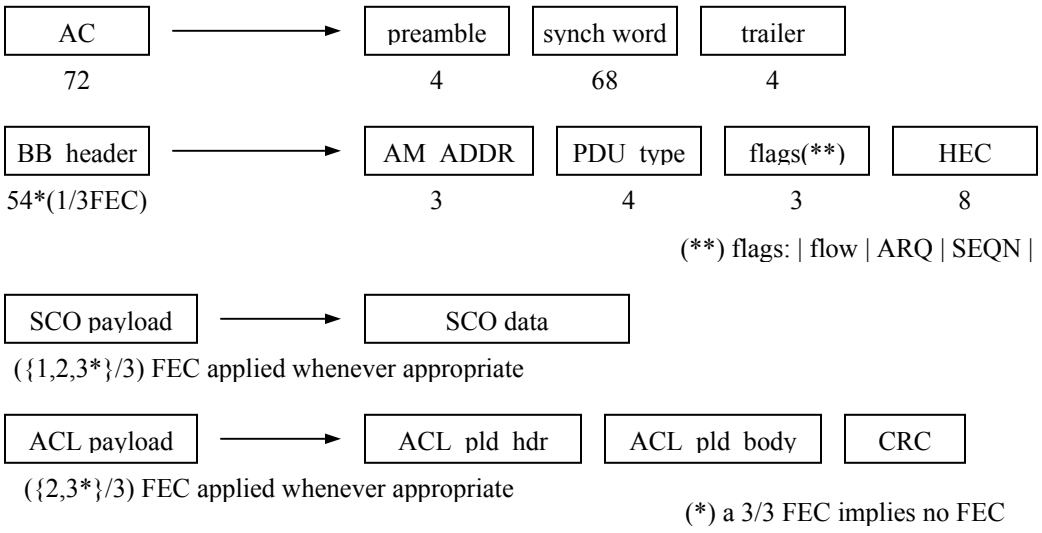


**Figure 4. Baseband Packet Fields [2]**

The ACL payload (Figure 5) consists of a header (ACL_pld_hdr), the body (ACL_pld_body), and a 16-bit cyclic redundancy check (CRC). The header contains a logical channel (L_CH) field for the transmission. If L_CH = b'11' the body "is passed to the link manager and is used for the configuration of the Bluetooth link"[2]. For L_CH = b'01' or b'10' L2CAP is the recipient of the body.

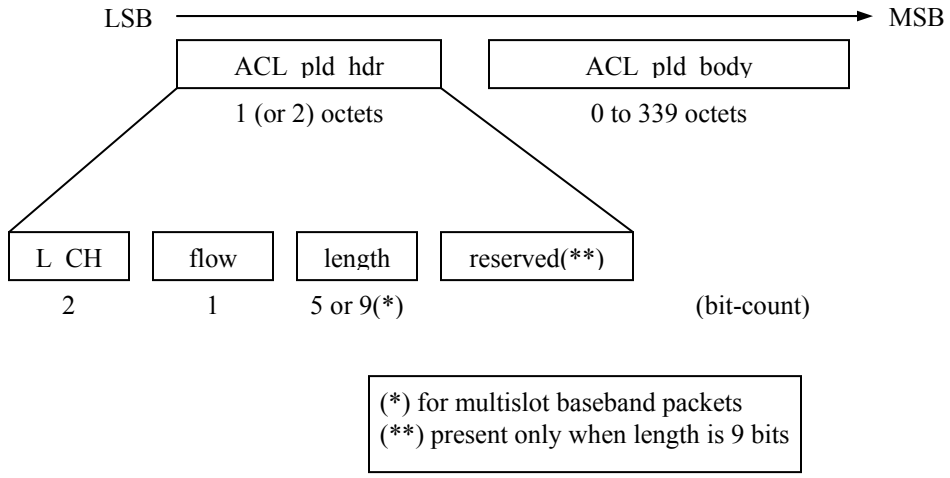


**Figure 5. ACL Packet Payload Format [2]**

#### 2.3.1.3 Link Manager Protocol

The Link Manager Protocol (LMP) handles link management. LMP is a transactional protocol that sets up the properties of a Bluetooth link. A "device may authenticate another device through a challenge/response mechanism" [2]. Once a device has been authenticated, the link between them may be encrypted. The link managers of different devices negotiate with each other to learn the other's features. The LMP is used to establish SCO connections, polling intervals, and packet sizes for transmissions between two devices.

One-slot ACL packets (c.f., Figure 6) with logical channel *L_CH* = b'11' carry the LMP packets. The LMP packet header is 8-bits in length with the first bit signifying the transaction ID (*tr_ID*). The *tr_ID* = b'0' if the master is the initiator and b'1' if the slave initiated the transaction.

Authentication and encryption algorithms both reside in the baseband, but the act of authenticating and encrypting are part of the LMP. Authentication "is based on a challenge/response mechanism based on a commonly shared secret, a *link key* generated through a user-provided PIN" [2]. Anytime throughout the duration of a connection a device may authenticate with another. It is initiated by one device transmitting an LMP challenge packet. The *challenger* generates a random number that is included in the challenge packet. The *claimant* receives the packet and operates on it using an authentication key of 128-bits. The claimant then returns the result to the challenger who compares it with the expected outcome. A correct comparison verifies the identity of the claimant.

After authentication the link may be encrypted to further enhance the security of the link. The linked Bluetooth devices generate a sequence of encryption keys from the link key. "The encryption key changes with each packet transmission" [2]. Depending on the government regulation for the country where the Bluetooth devices are operating, the encryption key may be as large as 128 bits. The SAFER+ algorithm is used to generate both the encryption and authentication keys. If a link is encrypted, both asynchronous and synchronous transmissions are encrypted.

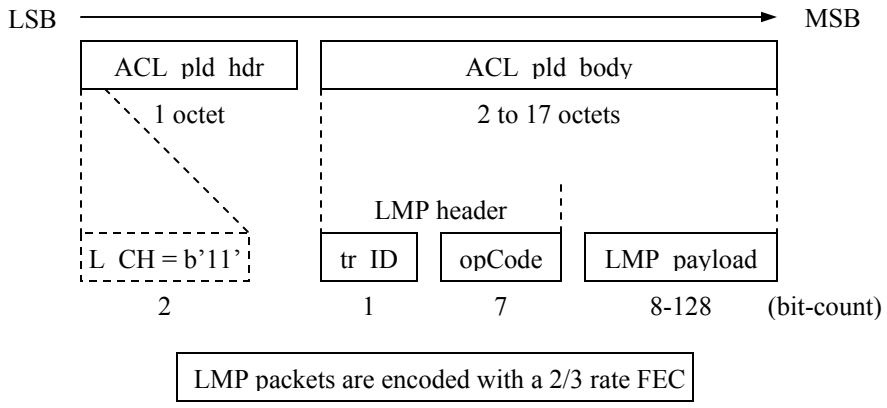


**Figure 6. LMP packet format [4]**

Low power modes for a Bluetooth device also reside in the baseband, but are configured and activated through LMP transactions. The low power modes for a Bluetooth device are the *sniff*, *hold*, and *park* modes. Sniff mode is the state of a slave who listens for a master transmission periodically per an agreement with the master. LMP transactions are used to configure the exact period between listenings. The hold mode is used when "a device agrees with its communication partner in a piconet to remain silent for a given amount of time" [2]. A holding device maintains its active member address, *AM_ADDR*.

In park mode the slave device relinquishes its *AM_ADDR*. The slave device is then silent until notified by the master that it can rejoin the piconet. The slave listens periodically for a beacon transmission broadcasted by the master. If the slave wants to unpark and rejoin the piconet it sends "a message to the master in the slots following the beacon instant" [2]. Even though the device is in a low power mode it can still accomplish other operations, thus low power mode only limits transmissions within a particular piconet.

#### 2.3.1.4 Host Controller Interface

The Host Controller Interface (HCI) resides between the lower layers of the Bluetooth stack and the host device. The HCI is not a protocol, but an interface used by the host device to send data intended for or receive data from other Bluetooth devices. Link creation to specific devices, inquiry execution, authentication requests, low power mode activation and so forth can be accomplished by the host device though the HCI. "The HCI provides a uniform command method of accessing the Bluetooth hardware capabilities" [4]. In general terms, the only way to talk to the hardware is through the HCI command set. The capabilities of the hardware available to applications are limited to those provided by the HCI.

#### 2.3.1.5 Logical Link Control and Adaptation Protocol

Just above the HCI in the Bluetooth protocol stack is the Logical Link Control and Adaptation Protocol (L2CAP). The implementation details of the lower layer are hidden from the higher layers by the L2CAP. "At the L2CAP layer, the concepts of master and slave devices" [2] no longer exist. Multiple logical channels are multiplexed over the ACL links of a device via the L2CAP. Hence, a master device can communicate

with multiple slaves within its piconet. L2CAP provides no support for SCO links. Audio transmitted over an SCO link is sent directly to the baseband layer.

Segmentation and reassembly of large L2CAP packets is supported. L2CAP packet format is shown in Figure 7. If a packet is segmented, the *L_CH* field of the ACL_pkt_hdr is set to b'10' to identify the first segment and b'01' for the rest of the segments.

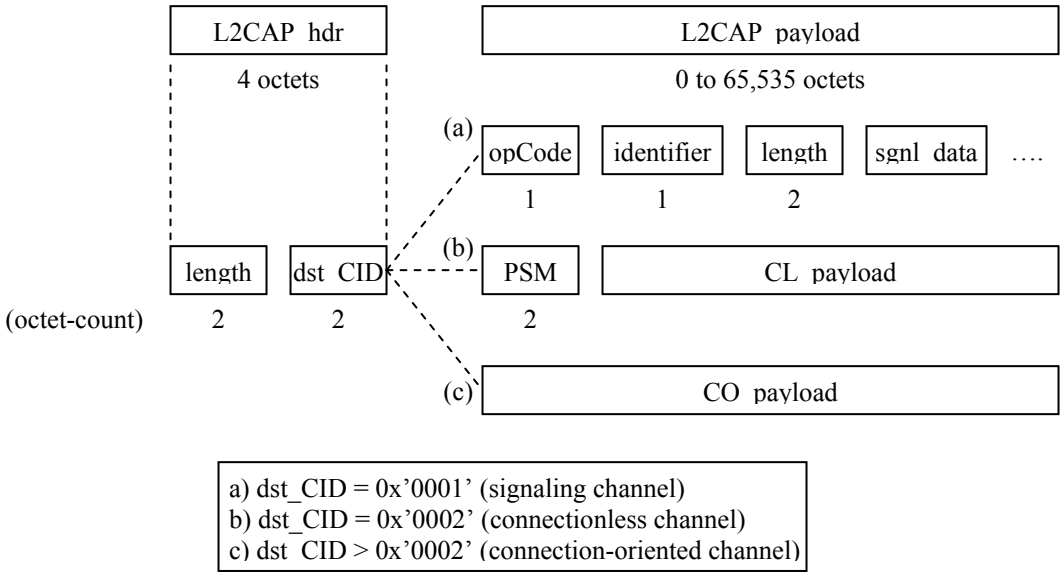


**Figure 7. L2CAP Packet Format [2]**

Traffic flow for the L2CAP is over logical connectionless or connection-oriented channels. Each channel has a two-octet *channel identifier* (CID) that is unique within each device. A CID of 0x'0001' identifies the signaling channel for a connection-oriented channel. CID value 0x'0002' is reserved for the connectionless channel.

Each L2CAP packet consists of a 4-octet header (L2CAP_hdr) and a payload section of up to 65,535 octets depending on the capabilities of the host device. L2CAP packets have three different payload formats depending on the CID. For signaling packets the payload is separated into four fields identified in Table 4.

**Table 4. L2CAP Signaling Packet Payload**

| Field | Length | Purpose |
|---|---|---|
| opCode | 1 octet | Identify the particular signaling data |
| indentifier | 1 octet | Match requests and responses |
| length | 2 octets | Length of data field |
| signaling data (sgnl_data) | Defined by previous length field | Contains the signaling data |

A connectionless L2CAP packet consists of a *PSM* field used for "protocol multiplexing in L2CAP channels" [2]. The *PSM* field is incorporated into the signaling data of a connection request for connection-oriented channels.

### 2.3.2 Middleware Protocols

#### 2.3.2.1 Service Directory Protocol

Bluetooth is designed to support a multitude of applications. In order for devices to determine what another device has to offer a Service Discovery Protocol (SDP) is utilized. Devices can inquire each other to determine what services are offered on the device and how to access them. No services can be accessed directly through the SDP; it is solely an information provider. A universally unique identifier (UUID), typically 128 bits in length, identifies each service and its attributes. Smaller 16-bit and 32-bit UUIDs may be used for known services.

#### 2.3.2.2 Radio Frequency Communication

The RFCOMM protocol provides serial line emulation based on the ETSI 07.10 specification [4]. RFCOMM "emulates RS-232 control and data signals over the Bluetooth baseband" [11]. This allows legacy applications that use serial lines as their transport mechanism to operate unmodified on a Bluetooth link.

#### 2.3.2.3 Telephony Control Signaling

The Telephony Control Signaling (TCS) protocol consists of the AT command set (TCS-AT) and Binary (TCS-BIN). RFCOMM enables use of the AT command set since they are designed to be passed over serial lines. Through AT commands a mobile phone or modem can be controlled. TCS-AT is based on ITU-T Recommendation V.250 and ETS 300 916 (GSM 07.07). TCS-BIN is a binary encoding of information "that runs directly on top of L2CAP" [4] and "supports normal telephony control functions such as placing and terminating a call, and sensing ringing tones" [2]. Additionally, TCS-BIN handles point-to-multipoint communication.

#### 2.3.2.4 Adopted Protocols

Bluetooth supports additional industry standard protocols including point-to-point (PPP), transport control protocol/internet protocol (TCP/IP), IrOBEX, and WAP [2]. Thus, Bluetooth is a very flexible specification designed to support new as well as legacy applications and provide flexible communication between many devices.

### 2.4 Wireless Security Issues

Security is important in any network and includes the following areas: *availability, confidentiality, integrity, authentication,* and *nonrepudiation*.

- *Availability* of a network describes on the survivability of network services even when under a denial-of-service attack. A denial-of-service attack may be employed against any layer of a network from physical jamming to routing protocol disruption to crashing high-level services.

- "*Confidentiality* ensures that certain information is never disclosed to unauthorized entities" [6]. Sensitive information that is transmitted requires confidentiality because the information might be valuable to an enemy.

- *Integrity* ensures that a transferred message is not corrupted. Corruption can occur due to benign failures or due to malicious attacks.

- *Authentication* guarantees identity of peers on a network. An adversary may masquerade as another node thereby gaining "unauthorized access to resources and sensitive information" [6] or interfering with other nodes on the network.

- *Nonrepudiation* prevents the sender of a message from denying that they ever sent the message.

Security in a wireless environment presents certain challenges. Wireless networks are "susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay, and message distortion" [6]. An eavesdropping adversary may gain access to private information violating confidentiality. Through active attacks, an adversary may delete messages, send erroneous messages, modify data, or impersonate a node. This violates availability, integrity, authentication, and nonrepudiation.

In order to ensure survivability, a network needs to be distributed in nature. Central control points in a network introduce a significant vulnerability. Wireless networks can also be dynamic in nature where frequent changes in membership of a network and the overall topology occur on a regular basis. Trust between nodes moving in and out of different networks is an important issue. Security of a wireless network must take all of these items into account in order to provide a robust defense.

## 2.5 Bluetooth Security Issues

Bluetooth has some basic weaknesses in security [9]. These vulnerabilities fall into the following categories: Eavesdropping and Impersonation, Location and Correlation, and Cipher Vulnerabilities.

### 2.5.1 Eavesdropping and Impersonation

Eavesdropping and Impersonation attacks both rely on capturing the initialization key used to encrypt and decrypt link key generation protocol information. The

initialization key is computed using a PIN, a random number, and the claimant's Bluetooth address. The claimant's address and the random number are both transmitted in the clear. The attacker will know the PIN if a default PIN of zero is used or if the PIN is transmitted in the clear. Otherwise, the attacker needs to perform an exhaustive search of all possible PINs (feasible if a medium or small length PIN is used).

Offline PIN crunching can be used in two scenarios. In the first "the attacker exhaustively guesses all PINs up to a certain length" [9]. The attacker then validates the guess is correct by performing the initialization key protocol verification step. This process is repeated until a correct result is found. This attack is referred to as eavesdropping.

For the second scenario, stealing by participation, the attacker begins with one PIN guess and performs the first part of initialization with the victim. The attacker then initiates the first round of the challenge-response protocol. The challenge-response transcript is then used to verify the guessed PIN. The attacker repeats verification until a guessed PIN outputs 'correct'. The key establishment protocol then continues with the verified PIN. Bluetooth uses an exponential back-off method to counter PIN guessing, but this only provides the attacker with more time to generate and verify PINs.

Both the link and optional encryption keys are generated from the initialization key so the initialization key security is crucial. In low memory mode, the unit key of a device is used as the link key. Thus, an attacker may be able to obtain a device's unit key via one of the above methods or by initiating contact with the device. Once a device's unit key is discovered, the attacker can impersonate the device and get the resulting link key.

Once an attacker has obtained the link key used by two devices, the attacker may perform a man-in-the-middle attack. The attacker contacts both devices that have completed communication using the aforementioned link key and establishes new link keys with both of them. Both of the previously communicating devices think they are talking to each other again and that the other started the session. The attacker negotiates with both to become masters or slaves. Both devices must be the same (master or slave) in order for the attacker to communicate with them since they must follow different hop sequences. Hence, the two victim devices will not see each other's transmissions. The attacker is now impersonating two devices to each other.

### 2.5.2 Location Attacks

Devices in discovery mode respond to inquiries with their *BD_ADDR*. Thereby, "an attacker can determine the location and movements of victim devices by maintaining geographically distributed devices that continuously inquire all devices entering within their reach, and recording the identities given in the response" [9]. If a Bluetooth device owner's identity is known, it can be tied to the device identity. Since the *BD_ADDR* is a permanent address assigned at the time of manufacture, an attacker can determine their movements and associations with other devices with a certain level of certainty.

Given that a device switches between different modes (*sniff*, *hold*, and *park* modes) in the application layer (namely the LMP) an attacker may take control of a victim's Bluetooth device through corrupt software (or some other means) and induce the device to scan for other devices in its area. Thus, the victim device will reveal its identity to these devices as it moves through their transmission range.

The master using its own BD_ADDR deterministically computes the Channel Access Code (CAC) for each channel. An attacker "listening on the baseband can determine the CAC associated with each (intercepted) message" [9]. Victims can then be indexed by their CACs and the relationship between device identifiers and CACs can be determined.

### 2.5.3 Hopping Along

Bluetooth conversations within a piconet frequency hop over 79 bands in the USA (23 bands in Spain and France). An attacker must listen to each and every band at the same time or hop synchronously with the master and slave holding a conversation. For an attacker to hop synchronously it must first identify the seed used for generating the hop sequence.

How the seed is generated depends on the device state. "In the inquiry (page) substate, the seed is deterministically derived from the inquiring device's own clock and the general inquiry access code" [9] (GIAC common to all devices). This differs from the connection substate where the master's clock and *BD_ADDR* determine the seed. Thirty-two (32) dedicated bands are used for inquiry and a responding device transmits its clock and *BD_ADDR*. An attacker can scan the inquiry bands and eavesdrop on the response messages. Furthermore, the master transmits its clock and *BD_ADDR* during paging, thus allowing the attacker to determine the hopping sequence seed.

### 2.5.4 Cipher Attacks

The encryption cipher is generated using the "encryption key $K_C$, the 48-bit *BD_ADDR*, the master clock bits $CLK_{26\text{-}1}$, and a 128-bit RAND value" [4]. Four linear

feedback shift registers (LFSR) of size 25, 31, 33, and 39 bits are loaded with an initial value derived from the four above inputs. From these the cipher is computed.

"An attacker can guess the content of the registers of the three smaller LFSRs and the summation register with probability of $2^{-93}$" [9]. The contents of the 39-bit register can be reverse engineered from the output to the others. Actual and generated outputs are compared to ascertain the correctness of the guess. This requires approximately 128 bits of ciphertext and known plaintext that can be obtained easily (sending a message to a phone and eavesdropping on the transmission to a headset). "Reverse engineering and verification takes approximately $2^7$ bit operations, making the total complexity of the attack $2^{100}$, which is less than the complexity of $2^{128}$ encryptions for a brute force attack" [9]. Only one frame is transmitted per key, thus the key is only good for that frame. By applying the attack twice, the master key can be obtained since the frame key is computed in the same manner as the sequence.

## 2.6 Summary

This chapter reviewed several topics necessary for a fundamental understanding of Bluetooth. First, wireless communications and the IEEE 802.11 family of standards were discussed. Additionally, transmission methods such as spread spectrum are introduced. Second, Bluetooth and its protocol stack were discussed in detail. Third, security issues for wireless communication were outlined. Finally, currently known Bluetooth specific security issues were discussed. The next chapter defines the experiment methodology.

# *3. Methodology*

## 3.1 Introduction

This chapter discusses the problem definition, specific research objectives, and a solution methodology. First, the problem definition is discussed including the reason for this research. Second, the objectives are presented followed by discussion of the Linux script developed. Finally, a solution methodology is presented in detail to include the system boundaries and parameters, evaluation technique, and experiment design and validation.

## 3.2 Problem Definition

DoD and Air Force installations continually incorporate new technology into the workplace to improve effectiveness and efficiency. Office devices utilizing Bluetooth technology simplify device configuration and communication. However, the Bluetooth protocol has security weaknesses as discussed in Chapter 2. Although these security weaknesses are not easily exploited, they are a cause for concern. When a weakness cannot be eliminated, it must be managed to minimize the possible effects of its exploitation.

The simplest way to manage the security weaknesses of the Bluetooth protocol is to minimize the possibility of packet transmission interception. This is accomplished by limiting the physical radius of transmission to within the boundaries of a controlled area. If transmissions are not receivable outside the controlled area, and the personnel and equipment within the controlled area are trusted, then the possibility of unauthorized packet interception is minimized. Thus, the need for defined transmission reception ranges of Bluetooth piconets is clear.

Currently there are multiple software programs for IEEE 802.11b that capture packets and map the reception ranges of multiple transmitters. This same functionality is desired for the Bluetooth protocol. Initially the Bluetooth experiments modeled those performed for the analysis of IEEE 802.11b. As an older standard, many different applications exist for the capture and analysis of 802.11b traffic. Kismet is one such application.

Kismet (**http://www.kismetwireless.net**) is a packet-capture application (i.e. a sniffer) that intercepts and records all packets it receives. This is accomplished passively. That is, no transmissions by the monitoring hardware are made. Additionally, Kismet provides the ability to record the GPS coordinates where the packet is intercepted and also records the power level of the received transmission. With this information, Kismet maps the power level of intercepted packet transmissions and displays them on screen in zones (red, yellow, and green) indicating the received power levels. The received power level correlates to an expected bit error rate based on the type of keying used for the transmission.

The original focus of this research was to develop a capability similar to Kismet for Bluetooth transmissions. After further analysis of the Bluetooth protocol and comparison to the IEEE 802.11b standard, it became clear that this could not be accomplished within the time allocated for this study. The following discussion is a summary of the findings that precluded the implementation of a Kismet-like tool for Bluetooth during this investigation.

First, to receive Bluetooth transmissions, the receiver must synchronize to the frequency hopping sequence of the piconet master. This differs from an 802.11b

transmission, which does not require explicit synchronization with a master. Each channel in 802.11b uses the same spreading sequence so a sniffer need only listen to a particular channel to intercept the packet transmissions. For a Bluetooth packet transmission, the exact frequency of transmission is only known if the frequency hopping sequence of the master is known. Thus a receiver cannot synchronize and listen in if it does not have the information needed, namely the *BD_ADDR* and clock of the master as discussed in Chapter 2. If the monitor wishes to remain passive, a method for determining the frequency hop sequence of the master without active participation in the piconet needs to be developed. This is not the focus of this study and is left as a follow-on research topic.

Second, according to the Bluetooth specification, the functional distance of a Level 3 Power Class Bluetooth transmitter is 10 m. This is much less than the range of 802.11b transmissions. The IEEE 802.11b transmissions are dependent on antenna type and can reach distances of more than a mile. Furthermore, the accuracy of a GPS unit is typically less the 15 m (3-5 m for Differential GPS (DGPS)). Thus, the use of GPS coordinates for tracking Bluetooth transmissions is not reasonable within the context of this study. Table 5 lists the power classes of Bluetooth devices and their respective output power levels.

**Table 5. Bluetooth Transmission Power Classes [4]**

| Power Class | Maximum Output Power (Pmax) | Nominal Output Power | Minimum Output Power | Power Control |
|---|---|---|---|---|
| 1 | 100 mW (20dBm) | N/A | 1 mW (0 dBm) | Pmin<+4 dBm to Pmax<br>Optional:<br>Pmin to Pmax |
| 2 | 2.5 mW (4 dBm) | 1 mW (0 dBm) | 0.25 mW (-6 dBm) | Optional:<br>Pmin to Pmax |
| 3 | 1 mW (0 DbM) | N/A | N/A | Optional:<br>Pmin to Pmax |

Third, 802.11b hardware has the capability to return power level values for the received signal. This capability is used by Kismet to track the power of intercepted packets. The Bluetooth hardware, specifically the baseband and radio layers, are accessed through the Host Controller Interface. The Bluetooth specification defines a basic command set that the interface provides (some chipset manufacturers provide additional commands specific to their hardware). The only function dealing with received power level is the optional implementation of the Receiver Signal Strength Indicator (RSSI). The RSSI does not return an explicit received power level value. The RSSI returns an approximation of the transmission deviation from the Golden Receive Range (c.f., Section 3.3.4). This RSSI is primarily for Bluetooth transmitters that incorporate power control and can vary transmission strength in response to a receiver request to increase or decrease power.

Given these limitations, it is not feasible to pursue development of Bluetooth capture software similar to Kismet. This is not to say that it cannot be accomplished, but it is outside the scope of this study.

The low transmission power of Bluetooth devices limits the range over which two devices can communicate. The 10 m range in the Bluetooth specification is assumed to be a maximum line-of-sight distance between two devices. It cannot be assumed that this is the maximum distance at which Bluetooth transmissions can be reliably received or intercepted. As the use of Bluetooth increases, more and more information will be communicated wirelessly and the need for securing that information becomes more pronounced.

### 3.3.1 Research Objectives

The primary objectives of this study are to determine the following:

1. The transmitter/receiver antenna orientation that provides the best reception for a commonly used configuration.
2. The ranges at which fixed levels of throughput can be received.

It is expected that the received signal power will decrease as the distance between the transmitter and receiver increases. This power decrease is due to path loss and destructive interference caused by reflected transmission signals. It is expected that changing the relative orientation of the receiver and transmitter antennas will cause an increase or decrease in the received signal power; this is dependent on which orientation is used for the initial measurement. Increasing distance is expected to decrease the throughput level. This decrease is due to path loss, and hence bit errors are likely to be in the signal. The decrease in throughput is not expected to occur at the same rate as received signal power within Bluetooth's specified 10 m functional range. Instead, the throughput should gradually decrease with more dramatic decreases at greater separation distances.

To achieve the research goals of this study, a Linux script is developed to utilize the functionality provided by the HCI for accessing the RSSI. Measurements of RSSI and throughput for transmissions in a free-space environment are recorded. This data is analyzed to determine the correlation between received power level, antenna orientation, and throughput range.

### 3.3.2 System Boundaries

The System Under Test (SUT) consists of those components required for wireless communication. These components are a transmitter, a transmission medium, and a

receiver, as shown in Figure 8. Data packets are sent to the transmitter and constitute the offered load. The transmitter places the packet onto the medium. The medium carries the packet transmission to the receiver. The receiver receives the packets and sends them out of the system. The Components Under Test (CUTs) are the transmitter antenna, the transmission medium, and the receiver antenna. The transmission medium is assumed to be free-space.

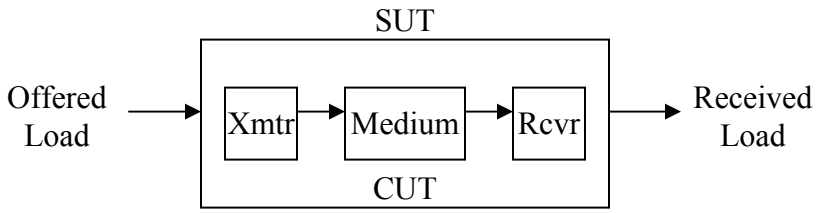


**Figure 8. System and Component Under Test**

This study is limited to only considering relative antenna orientation in 90-degree increments. Additionally, the study is limited to outdoor transmissions and free-space propagation. The transmission power level is set at 1 mw. It is infeasible to determine ranges for every Bluetooth communication mode. Therefore, the experiment is limited to File Transfer Protocol (FTP) traffic using the Data Medium rate 5-slot (DM5) packet type. This packet type has a theoretical maximum forward (asymmetric) throughput rate of 477.8 kbps [3]. Additionally, it is assumed that there is no interference due to other transmissions.

### 3.3.3 System Services

The system provides one service – wireless transmission of data from a transmitter to a receiver. The possible outcomes of this service are success and failure. A successful outcome occurs when the received transmission is error free or is

correctable by the FEC or CRC. Everything else is a failure. Failure consists of the following possibilities:

- No transmission is received – the signal power level is below a certain reception threshold (threshold varies vendor to vendor), or
- Transmission is received, but with errors – errors beyond the correction capability of the FEC or CRC

### 3.3.4 Performance Metrics

The performance metrics are throughput and RSSI. The size of the data (in bits) divided by the total time taken to receive the data defines throughput. Throughput provides a measure of network capacity and indicates how many transmissions can be successfully sent under a given set of circumstances.

The Received Signal Strength Indicator (RSSI) is an optional capability for transceivers to support power-control links. It provides the means "to measure the strength of the received signal and determine if the transmitter on the other side of the link should increase or decrease its output power level" [4].

Each Bluetooth receiver has a Golden Receive Range defined by two thresholds. The lower threshold "corresponds to a received power between –56 dBm and 6 dB above the actual sensitivity of the receiver" [4], which is defined as a minimum of –70 dBm with a raw bit error rate (BER) of $10^{-3}$. The upper threshold falls in the range of 14 dB to 26 dB above the lower threshold as depicted in Figure 9.

The RSSI value is a whole number indicator in decibels (dB) of the approximate location (above or below) of the received signal strength relative to the Golden Receive Range. When the received signal strength is within the Golden Receive Range, the RSSI returns a value of zero. "The Golden Receive Power Range is normally around 20 dBm wide, crudely equating to a physical range factor of ten" [5]. Thus, the returned RSSI

value can be zero for transmissions in the range of 1 m to 10 m. This corresponds to the 10 m operational range of Bluetooth devices as outlined in the specification.

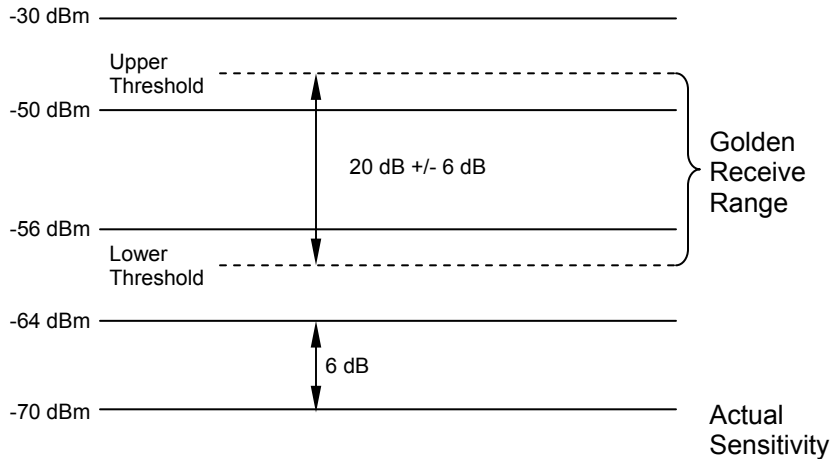


**Figure 9. RSSI Dynamic Range and Accuracy**

The RSSI returns a positive or negative value only when the received signal strength is outside of the Golden Receive Range. A positive value indicates the received signal power is above the Golden Receive Range, while a negative value indicates the received signal power below the Golden Receive Range. Positive values are approximate decibel (dB) values between the upper Golden Range threshold and the actual received signal strength. Negative values are approximate decibel (dB) values between the actual received signal strength and the lower Golden Range threshold. All RSSI values are approximate and "can be more than ±5 dB from the real value" [5]. Negative values are clipped to a minimum of –10 dB for CSR chipsets and –15 dB for Ericsson chipsets.

### 3.3.5 Parameters

System parameters for this experiment are as follows:

- Temperature – Temperature inversion can cause reflection of radio waves and signal loss

- Humidity – Attenuation due to the density of water in the air, this is due to the close proximity of the transmitted frequency to the resonance frequency of water molecules

- Wind – Wind can cause constant changes in air temperature and humidity thus leading to unpredictable signal loss

- Antenna orientation – The antenna gain pattern (directivity) may affect received signal power and throughput

- Transmitter distance from receiver – The path loss due to propagation through free-space lowers signal power and may hinder reception

- Electromagnetic interference (EMI) – Both natural and man-made EMI can occur, such as transmissions at the same frequency by other broadcasting radio devices, microwave ovens, and radiation

Workload parameters are as follows:

- Packet type – The theoretical throughput limit of transmitted DM5 packets is 477.8 kbps in a piconet having only a master and one slave. Different packet types have an effect on the throughput

### 3.3.6 Factors

The factors and corresponding values for this experiment are:

- Antenna orientation – (90-degree, 180-degree, 270-degree, and 360-degree) – Transmitter/receiver antenna orientations are selected based on the minimum number of different orientations needed to measure 360-degrees around the transmitter or receiver

- Transmitter distance from receiver – (1 meter increments for RSSI until lower threshold is reached, 5 meter increments for throughput with 1 meter refinements) – Distances for RSSI measurement are based on the narrow range over which the RSSI is expected to be useful. Distances for throughput are based on initial rough measures and refined as needed

The antenna orientations selected reflect the different axis in a two-dimensional plane. It is expected that the gain of the micro-strip patch antenna is not equal in all directions. It is expected that orientations aligning the primary lobes will produce the best RSSI values and throughput rate.

The distance between the transmitter and receiver is expected to be the primary contributor to the decrease in RSSI value and throughput rate. This is due to transmission path attenuation.

### 3.4.1 Evaluation Technique

The experiment is conducted using direct system measurement. This technique is selected due to the unknown nature of the effects of the factors and the availability of a Bluetooth testbed. Direct measurement of Bluetooth transmissions provides the simplest means for determining a possible correlation between the factors and the performance metrics. Measurement also provides the most accurate representation of real world scenarios.

The results of implementing a measurement technique will be validated using the path loss analytical model for radio frequency transmissions in open-air. The analytical model provides an easy, quick, low-cost method for validating the measurements. The lower accuracy of the analytical model eliminates it from being the primary evaluation method for this experiment. The accuracy of the analytical model is low due to the unknown nature of the environments the transmissions may occur in. It requires too many assumptions and simplifications to result in the desired level of accuracy.

### 3.4.2 Workload

The components under test are the transmission distance and the orientation of the antenna. The distance the signal travels is measured from the closest edge of the transmitting antenna to closest edge of the receiving antenna. The power level of the signal is set at 1 mw. For the orientation experiment, there is no load on the system. The RSSI command measures the signal strength of the current packet. In the orientation

experiment, a connection is established, but no data is sent during the test. The packets are limited to polling packets between the piconet master and slave.

For the throughput experiment, a 1001 KB JPEG file is sent from the transmitter to the receiver via the file transfer protocol. The file size of 1001 KB is selected simply for ease of throughput calculation and convenience (the file is already on hand). An approximately 1 MB file eases mental calculations of throughput estimates during the experiment execution. The size of approximately 1 MB provides enough time to determine an accurate throughput measurement. The theoretical minimum amount of time to transmit the file is $\frac{1001KB(8bits/byte)}{477.8kbps} = 16.76s$.

The file transfer protocol software accompanying the Bluetooth cards used in the experiments utilizes DM5 packets. A constant workload of DM5 packet transmissions provides a good means of measuring the throughput. The workload consists of DM5 packets broadcast until the file transfer is complete and acknowledged.

### 3.4.3 Experimental Design

The experimental design for the orientation experiment is a two factor full factorial design with replications. A two factor full factorial design allows separation of the interactions from experimental errors. Since RSSI values are integers, it is clear that the hardware is either rounding or truncating the actual signal strength. In order to give a better estimate of the difference between received signal strength and Golden Range threshold, 100 samples for each orientation and distance are averaged. The number of required experiments, *n*, using a two factor full factorial design with replications is:

$$n = abr = (4 \text{ orientations})(21 \text{ distances})(100 \text{ replications}) = 8400 \quad (1)$$

The advantage of this design is that every possible combination of configuration is examined. The effect of every factor and their interaction can be determined. Additionally, a confidence interval for experimental errors can be determined for a selected confidence level.

Each experiment consists of a unique combination of the factors and corresponding levels. A baseline RSSI lower threshold maximum range determination is made using free-space transmissions and the Bluetooth PC card manufacturer's original unmodified hardware. This range is the maximum range at which the RSSI value is above the lower threshold of –15 dB for the Ericsson chipset used.

The experimental design for the throughput experiment is a two factor full factorial design with replications. Since throughput is expected to decrease at different ranges for different orientations, the connection between the master and slave will fail and data will not be collected beyond that distance for that orientation. Thus, there is no way to compare results between orientations. Therefore, the best-case measurement is used. Each experiment is performed *r* times and the best result is selected as the sample value.

Although this is a best-case measurement, how close this measure is to the best-case mean is of interest. Assuming the errors are normally distributed, the number of replications, *r*, required is given by solving the mean confidence interval equation for *r*

$$\bar{x} \mp z\frac{s}{\sqrt{r}} = \bar{x}\left(1 \mp \frac{a}{100}\right) \tag{2}$$

$$r = \left(\frac{100zs}{a\bar{x}}\right)^2 \tag{3}$$

where $\bar{x}$ is the mean of the baseline sample, $z$ is the normal variate for the desired confidence level, $s$ is sample standard deviation, and $a$ is the desired accuracy of the confidence interval.

A baseline throughput measured in the lab at a distance of 2 m identified little variation between measurements (Table 6). The transmitter and receiver are both placed on desktops at a height of 0.6584375 m. Both the transmitter and receiver are placed at the 90-degree orientation with respect to each other.

**Table 6. Lab Sample Throughput Values**

| File Transfer Time (sec) | Calculated Throughput (kbps) |
|---|---|
| 26.46 | 302.63 |
| 26.53 | 301.75 |
| 26.62 | 300.73 |
| Mean = | 301.70 |
| Std. Dev. = | 0.77 |

A confidence level of 95% is selected since the throughput loss is high with respect to the change in distance compared to the throughput gain. This high loss is due to the short distance over which Bluetooth devices are designed to function. Choosing a confidence level of 95% gives $a = 5$ and $z = 1.645$.

Although the calculated number of replications required is less than one due to the small standard deviation in the measured throughput, three replications per measurement are performed.

### 3.5 Result Analysis and Interpretation

Once orientation data is collected, the effects of selected factors are quantified using ANOVA. The ratio of the Mean Square of factor x (MSx) and the Mean Square of Error (MSE) is calculated, where MSx is given by SSx divided by degrees of freedom and MSE is given by dividing the sum of squares for error by its degrees of freedom.

This ratio is compared to the F-distribution $F(n, m)$ using SSx degrees of freedom for n and SSE degrees of freedom for m. If MSx/MSE ≥ the $F(n, m)$ table value, the effect of factor x is statistically significant with respect to the error.

For either factor, if the confidence intervals overlap for different levels, then the number of replications of that experiment is increased. The number of additional replications is determined from the previously gathered data for that factor. By equating the lower bound of the higher factor level with the upper bound of the lower factor level and solving for number of observations, the number of additional replications needed to separate the overlapping confidence intervals is determined.

## 3.6 Summary

The experiment outlined in this chapter is intended to determine a preferred receiver antenna orientation. Then, using that orientation to determine ranges for fixed throughput levels. Factors considered include receiver antenna orientation and distance the signal travels. ANOVA is used to determine factor contribution to variation and determine confidence intervals of measured data.

It is expected that distance, rather than antenna orientation is the primary contributing factor to RSSI variation. As the distance between the transmitter and receiver increases, the RSSI value and throughput will decrease. The RSSI value decrease is expected to follow that of the path loss equation, whereas throughput will drop off slowly at first and more quickly at greater ranges. The orientation of the antenna is expected to contribute to the variation in measured RSSI values and throughput rate. Each orientation is expected to be significantly different, thereby indicating one as the

most appropriate. The next chapter discusses the experiments performed, the data gathered, and the data analysis.

# *4. Experiments, Data, and Analysis*

## 4.1 Introduction

This chapter discusses orientation and throughput experiments utilizing consumer level Bluetooth Compact Flash (CF) and PC cards as well as models developed to explain observations. First, the orientation experiment is discussed along with the data collected and data analysis. Second, the anomalies observed are presented followed by discussion of the interference model developed. Finally, the throughput experiment is discussed in detail to include a mapping of the ranges of throughput observed.

## 4.2 RSSI

Utilizing a pair of Armadillo Bluetooth CF Cards (Ericsson chipsets), the first experiment seeks to determine the effect of receiver orientation on the RSSI in a free-space environment. The transmitter orientation is kept constant while the receiver is placed in four different orientations at each distance. Distances are measured in one-meter increments in a straight line from the transmitter. The transmitter and receiver are supported by cardboard boxes at a height of 0.59055 m. A Linux script file (c.f., Appendix A) is used to sample the RSSI 100 times at each orientation and distance. Table 7 records the average values.

The Armadillo Bluetooth CF cards used in the experiment have an integrated microstrip patch antenna for transmissions. It is expected that the antenna orientation contributes to the RSSI value. The extent to which the orientation contributes to the variation in RSSI values is determined through computation of effects and Analysis of Variance (ANOVA) as described in [8].

**Table 7. RSSI Values (dB) for Experiment 1**

| | | Orientation (degrees) | | | |
|---|---|---|---|---|---|
| | | 90 | 180 | 270 | 360 |
| Distance (meters) | 1 | 0.00 | -2.66 | 0.00 | -3.34 |
| | 2 | 0.00 | -5.00 | 0.00 | -8.04 |
| | 3 | -5.43 | -8.50 | -5.81 | -12.74 |
| | 4 | -4.26 | -9.77 | -4.70 | -12.84 |
| | 5 | -6.98 | -13.36 | -11.38 | -13.56 |
| | 6 | -12.87 | -13.12 | -12.96 | -13.80 |
| | 7 | -13.22 | -11.90 | -12.52 | -15.00 |
| | 8 | -10.13 | -13.00 | -10.15 | -13.92 |
| | 9 | -10.30 | -12.80 | -10.70 | -15.00 |
| | 10 | -9.76 | -12.56 | -10.06 | -15.00 |
| | 11 | -10.79 | -13.24 | -10.85 | -15.00 |
| | 12 | -10.65 | -15.00 | -10.00 | -15.00 |
| | 13 | -11.06 | -14.08 | -11.13 | -15.00 |
| | 14 | -12.04 | -14.88 | -11.36 | -15.00 |
| | 15 | -12.16 | -14.80 | -12.10 | -15.00 |
| | 16 | -13.16 | -14.68 | -13.12 | -15.00 |
| | 17 | -14.46 | -15.00 | -13.00 | -15.00 |
| | 18 | -13.44 | -15.00 | -13.00 | -15.00 |
| | 19 | -13.38 | -15.00 | -14.78 | -15.00 |
| | 20 | -15.00 | -15.00 | -14.94 | -15.00 |
| | 21 | -15.00 | -15.00 | -15.00 | -15.00 |

### 4.2.1 Antenna Orientation

The orientation is measured with respect to the transmitter/receiver. The Bluetooth card is inserted on the right-hand side of the laptop when facing the screen. Figure 10 depicts the orientations of the patch antenna on the Bluetooth card when it is inserted in the laptop.

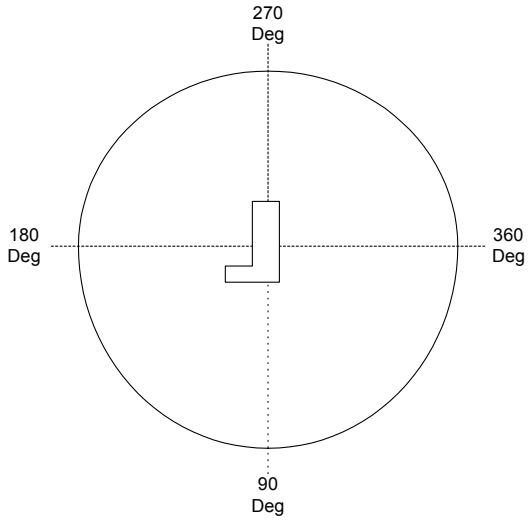


**Figure 10. Microstrip Patch Antenna Orientation**

### 4.2.2 Computation of Effects

The computation of effects shown in Table 8 is interpreted as follows. The mean distance with a mean orientation has an RSSI value of –11.72 dB. The RSSI value for the 90-degree orientation is 1.52 dB higher than that of an average orientation. The 270-degree orientation RSSI value is 1.36 dB higher on average than that of an average orientation. The RSSI value for the 180-degree orientation is 0.86 dB lower than that of an average orientation and the 360-degree orientation is 2.01 dB lower than that of an average orientation. The RSSI value for the 90-degree orientation is on average higher than any of the other measured orientations.

**Table 8. Computation of Effects for Orientation Experiment 1**

| | | Orientation (degrees) | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | 90 | 180 | 270 | 360 | Row Sum | Row Mean | Row Effect |
| Distance (meters) | 1 | 0.00 | -2.66 | 0.00 | -3.34 | -6.00 | -1.50 | 10.22 |
| | 2 | 0.00 | -5.00 | 0.00 | -8.04 | -13.04 | -3.26 | 8.46 |
| | 3 | -5.43 | -8.50 | -5.81 | -12.74 | -32.48 | -8.12 | 3.60 |
| | 4 | -4.26 | -9.77 | -4.70 | -12.84 | -31.57 | -7.89 | 3.82 |
| | 5 | -6.98 | -13.36 | -11.38 | -13.56 | -45.28 | -11.32 | 0.40 |
| | 6 | -12.87 | -13.12 | -12.96 | -13.8 | -52.75 | -13.19 | -1.47 |
| | 7 | -13.22 | -11.90 | -12.52 | -15.00 | -52.64 | -13.16 | -1.44 |
| | 8 | -10.13 | -13.00 | -10.15 | -13.92 | -47.20 | -11.80 | -0.08 |
| | 9 | -10.30 | -12.80 | -10.70 | -15.00 | -48.80 | -12.20 | -0.48 |
| | 10 | -9.76 | -12.56 | -10.06 | -15.00 | -47.38 | -11.85 | -0.13 |
| | 11 | -10.79 | -13.24 | -10.85 | -15.00 | -49.88 | -12.47 | -0.75 |
| | 12 | -10.65 | -15.00 | -10.00 | -15.00 | -50.65 | -12.66 | -0.95 |
| | 13 | -11.06 | -14.08 | -11.13 | -15.00 | -51.27 | -12.82 | -1.10 |
| | 14 | -12.04 | -14.88 | -11.36 | -15.00 | -53.28 | -13.32 | -1.60 |
| | 15 | -12.16 | -14.80 | -12.10 | -15.00 | -54.06 | -13.52 | -1.80 |
| | 16 | -13.16 | -14.68 | -13.12 | -15.00 | -55.96 | -13.99 | -2.27 |
| | 17 | -14.46 | -15.00 | -13.00 | -15.00 | -57.46 | -14.37 | -2.65 |
| | 18 | -13.44 | -15.00 | -13.00 | -15.00 | -56.44 | -14.11 | -2.39 |
| | 19 | -13.38 | -15.00 | -14.78 | -15.00 | -58.16 | -14.54 | -2.82 |
| | 20 | -15.00 | -15.00 | -14.94 | -15.00 | -59.94 | -14.99 | -3.27 |
| | 21 | -15.00 | -15.00 | -15.00 | -15.00 | -60.00 | -15.00 | -3.28 |
| | Column Sum | -214.09 | -264.35 | -217.56 | -288.24 | -984.24 | | |
| | Column Mean | -10.19 | -12.59 | -10.36 | -13.73 | | -11.72 | |
| | Column Effect | 1.52 | -0.87 | 1.36 | -2.01 | | | |

The 90% confidence intervals for effects in Table 9 shows that each orientation is significantly different from each other except for one case. The 90% confidence interval for the contrasts between the 90-degree orientation and the 270-degree orientation is (-2.26, 2.59). Since this confidence interval contains zero, the 90-degree orientation and the 270-degree orientation are not significantly different from each other. Hence, either orientation can be used for the throughput experiment.

**Table 9. 90% Confidence Intervals for Orientation Effects**

| Parameter | Mean Effect | Std Dev | Conf Interval | |
|---|---|---|---|---|
| Mean | -984.24 | 0.03 | -984.30 | -984.18 |
| Orientation | | | | |
| 90 | 1.52 | 0.06 | 1.42 | 1.62 |
| 180 | -0.87 | 0.06 | -0.97 | -0.77 |
| 270 | 1.36 | 0.06 | 1.26 | 1.46 |
| 360 | -2.01 | 0.06 | -2.11 | -1.91 |

### 4.2.3 Analysis of Variance

The ANOVA for Experiment 1 in Table 10 shows that distance accounts for the majority of variation (77.72%) in the RSSI values. This is expected simply due to path loss. The receiver antenna orientation accounts for 13.92% of the variation in RSSI value, while only 0.43% is accounted for by errors. The remaining 7.94% of variation is due to interaction between the factors (distance and orientation) in the experiment.

The *F*-ratio is used to test the significance of each factor. Utilizing the degrees of freedom (DOF) for orientation and distance, each factor's respective *F*-value is computed and compared to those contained in the table of quantiles of *F*-variates [8]. Each factor is significant at level $\alpha = 0.01$ (99-percentile) since the computed *F*-value is greater than the *F*-value from the table of quantiles.

Thus, the significance of receiver antenna orientation, as indicated by the *F*-ratio test, combined with the computation of effects, identifies the 90-degree and 270-degree receiver antenna orientations as the better receiver antenna orientations for future best-case scenario experiments.

**Table 10. ANOVA for Orientation Experiment 1**

| Component | Sum of Squares | Variation (%) | DOF | Mean Square | F-Computed | F-Table |
|---|---|---|---|---|---|---|
| y | 12883.44 | | 84 | | | |
| y.. | 11532.48 | | 1 | | | |
| y-y.. | 1350.96 | 100.00 | 83 | | | |
| Orientation | 188.00 | 13.92 | 3 | 62.67 | 643.62 | 4.31 |
| Distance | 1049.91 | 77.72 | 20 | 52.50 | 539.16 | 2.37 |
| Errors | 5.84 | 0.43 | 60 | 0.10 | | |

## 4.3 Signal Interference

When viewed graphically, it is clear that received signal strength does not decrease in a smooth manner as expected from theoretical path loss. Theoretical path loss shown in Figure 11 is calculated from the following equation:

$$\text{Path Loss} = 20Log_{10}\left(\frac{\lambda}{4\pi R}\right) \tag{4}$$

where λ is the signal wavelength and *R* is the signal propagation distance. Instead, signal strength attenuates markedly at approximately 3m and 6m as shown in Figure 12, especially for the 90-degree and 270-degree antenna orientations.

To determine whether this anomaly is due to experimental error even though not indicated by ANOVA, three additional experiments were performed. The second experiment consisted of a 3Com Bluetooth PC Card running on a Dell Inspiron 8200 under Windows 2000 as the transmitter and the same receiver configuration used in

Experiment 1. All other factors in the experiment were the same. Experiment 2, shown in Figure 13, shows the same attenuation in RSSI values at the same distances.

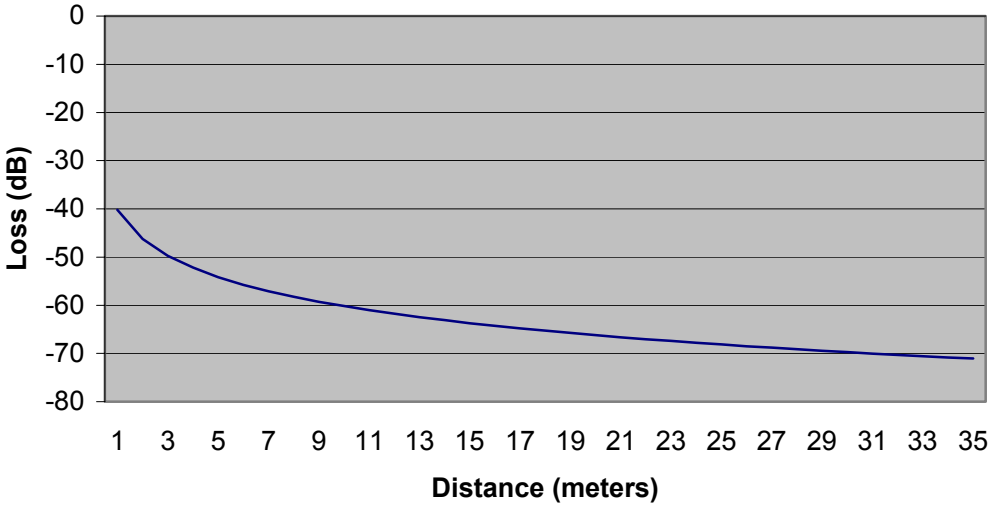


**Figure 11. Theoretical Free-Space Path Loss**

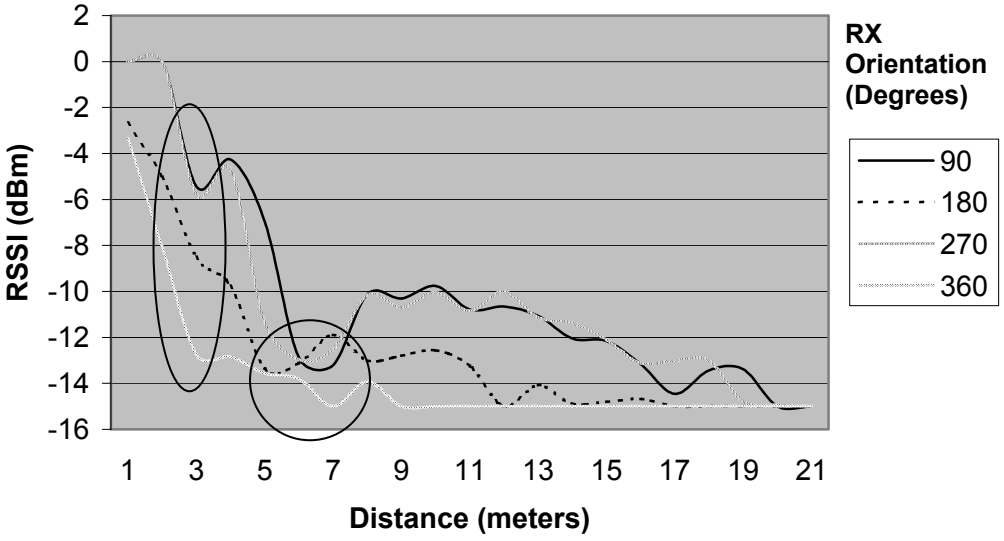


**Figure 12. RSSI Values for Experiment 1**

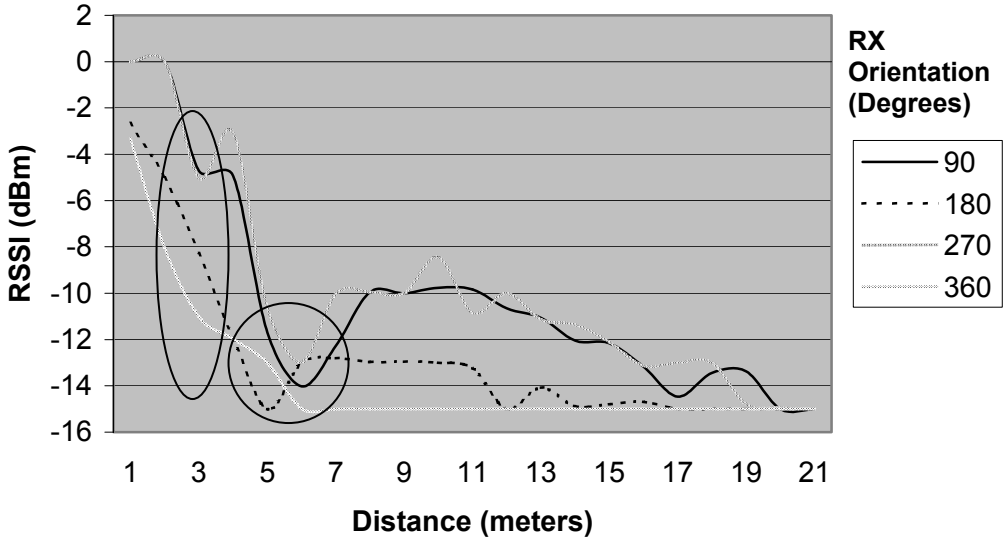


**Figure 13. RSSI Values for Experiment 2**

The third experiment consisted of a TDK Bluetooth PC Card running on a Dell Inspiron 8200 under Windows 2000 as the transmitter and the same receiver configuration from Experiment 1. All other factors in the experiment were the same. Experiment 3 results, shown in Figure 14, again reveal the same drop in RSSI values at the same distances.

To verify the results of the first three experiments, a fourth experiment was performed in which the transmitter orientation was varied and the receiver orientation held constant at 270-degrees. This orientation was previously found to have a strong received signal strength.

Results from Experiment 4, shown in Figure 15, indicate that the anomaly occurs regardless of orientation of transmitter or receiver. Although the RSSI is only an approximation, and can vary up to 5 dB within a range that is partially dependent on the chipset maker, the continual occurrence of the received signal strength drop off indicates

this is not likely a hardware issue, but caused by some fundamental property of Bluetooth transmissions.

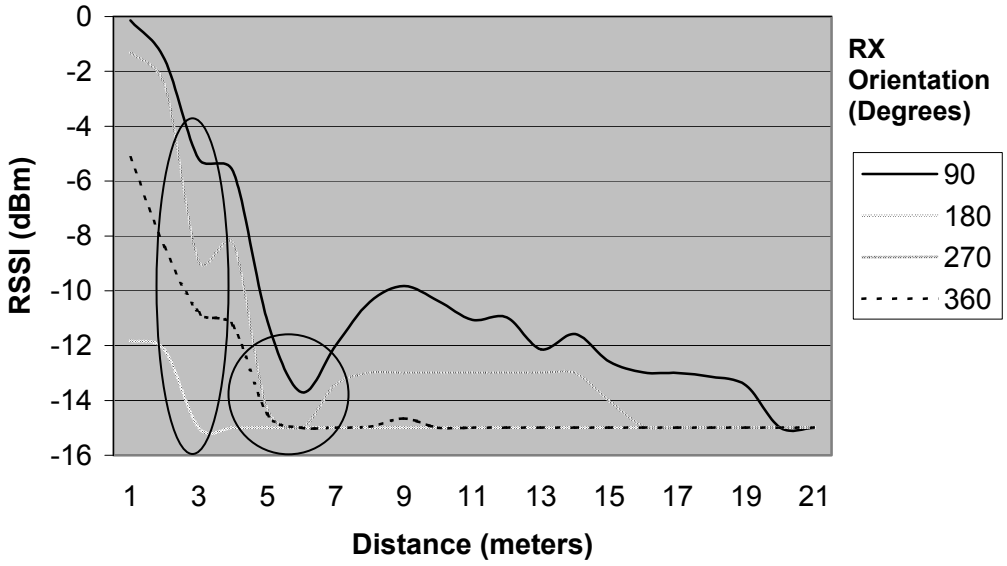


**Figure 14. RSSI Values for Experiment 3**

After further investigation, the cause for signal attenuation was determined to be destructive interference of a reflected signal superpositioned on the primary signal at the point of reception. This was verified through the construction of an analytical model identifying distances at which maximum destructive interference occurs.

For destructive interference to occur, a signal reflected from a planar surface within the region of the experiment is superpositioned with the primary signal. The reflected signal arrives 180 degrees out-of-phase with the primary signal and destructively interferes at all even numbered half-wavelength increments. The experiments are performed in an free-space environment where the only plane of reflection is the ground. Thus, the distance traveled by the reflected wave equals the distance traveled by the primary signal plus any even numbered half-wavelength.

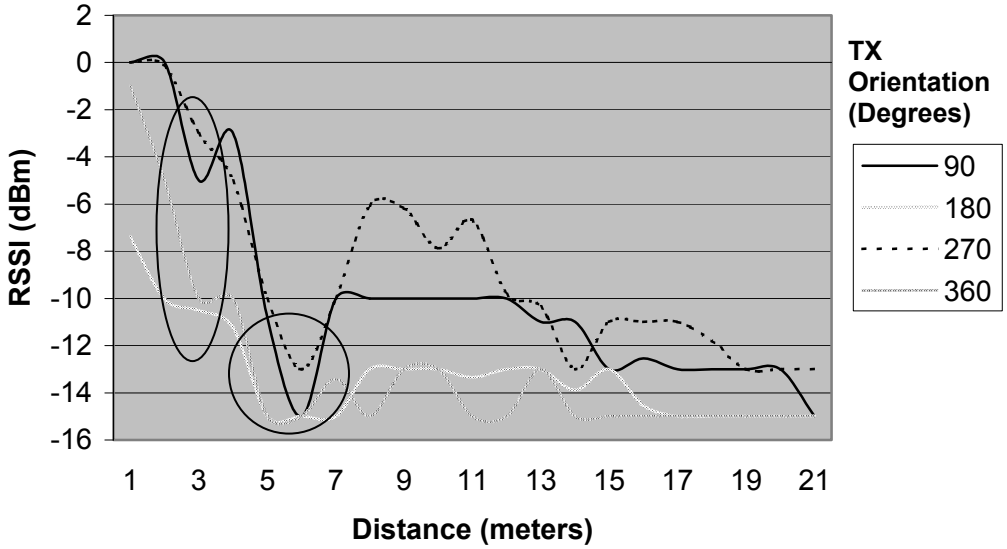


**Figure 15. RSSI Values for Experiment 4**

The geometry of Figure 16 is used for destructive signal analysis. Let the primary signal distance be the direct path distance, $R_D$, from the transmitting antenna, $A_T$, to the receiving antenna, $A_R$. The reflected signal distance is $R_1 + R_2$ where $R_1$ is the direct distance from the transmitting antenna, $A_T$, to the reflection point and $R_2$ is the direct distance from the reflection point to the receiving antenna, $A_R$. Then,

$$R_1 + R_2 = R_D + m\left(\frac{\lambda}{2}\right) \tag{5}$$

and destructive interference is at its maximum when $m$ is a positive integer.

Let the transmitting antenna height be $h_1$ and the receiving antenna height be $h_2$. Let $\Theta_1$ be the angle of incidence and $\Theta_2$ be the angle of reflection. For planar reflection, $\Theta_1 = \Theta_2$, since the angle of reflection equals the angle of incidence for any electromagnetic wave. Let the ground distance from the transmitter to the reflection

point be $l_1$ and the ground distance from the reflection point to the receiver be $l_2$. The total distance between the antenna bases, $R_B$, is then given by

$$R_B = l_1 + l_2 \tag{6}$$

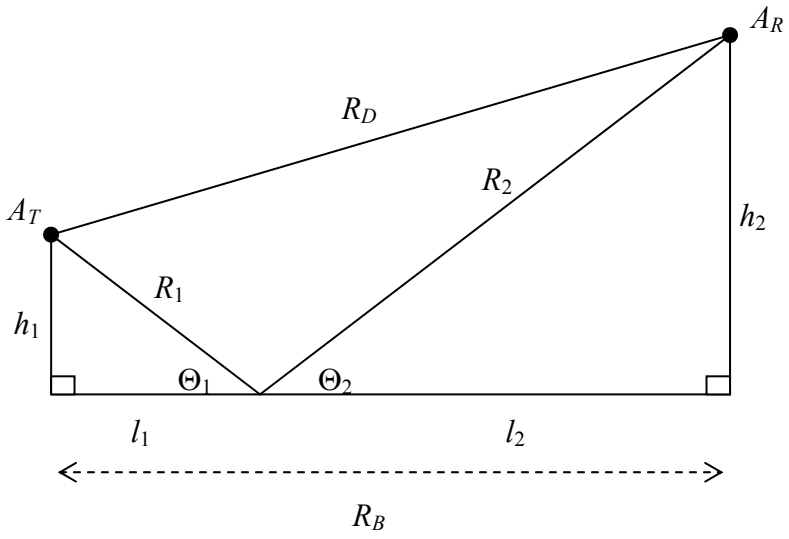


**Figure 16. Signal Propagation Model**

Since $\Theta_1 = \Theta_2$,

$$\tan\Theta_1 = \tan\Theta_2 \Leftrightarrow \frac{h_1}{l_1} = \frac{h_2}{l_2} \Rightarrow \frac{h_1}{h_2} = \frac{l_1}{l_2} \tag{7}$$

Solving for $l_1$ gives

$$l_2 = R_B - l_1 \tag{8}$$

$$\frac{l_2}{l_1} = \frac{R_B}{l_1} - 1 = \frac{h_2}{h_1} \tag{9}$$

$$\frac{R_B}{l_1} = \frac{h_2}{h_1} + 1 = \frac{h_1 + h_2}{h_1} \tag{10}$$

$$l_1 = \frac{h_1 R_B}{h_1 + h_2} \tag{11}$$

and solving for $l_2$ gives

$$l_1 = R_B - l_2 \tag{12}$$

$$\frac{l_1}{l_2} = \frac{R_B}{l_2} - 1 = \frac{h_1}{h_2} \tag{13}$$

$$\frac{R_B}{l_2} = \frac{h_1}{h_2} + 1 = \frac{h_1 + h_2}{h_2} \tag{14}$$

$$l_2 = \frac{h_2 R_B}{h_1 + h_2} \tag{15}$$

Solving for $R_1$, $R_2$ and $R_D$ gives

$$R_1 = \sqrt{h_1^2 + l_1^2} = \sqrt{h_1^2 + \left(\frac{h_1 R_B}{h_1 + h_2}\right)^2} \tag{16}$$

$$R_2 = \sqrt{h_2^2 + l_2^2} = \sqrt{h_2^2 + \left(\frac{h_2 R_B}{h_1 + h_2}\right)^2} \tag{17}$$

and

$$R_D = \sqrt{R_B^2 + (h_2 - h_1)^2} \tag{18}$$

Incorporating $R_1$, $R_2$, and $R_D$ into interference equation (5) results in

$$\sqrt{h_1^2 + \left(\frac{h_1 R_B}{h_1 + h_2}\right)^2} + \sqrt{h_2^2 + \left(\frac{h_2 R_B}{h_1 + h_2}\right)^2} = \sqrt{R_B^2 + (h_2 - h_1)^2} + m\left(\frac{\lambda}{2}\right) \tag{19}$$

For the RSSI experiments $h_1 = h_2$. Consequently, $R_D = R_B$ and $R_1 = R_2$, and (19) reduces to

$$2\sqrt{h_1^2 + \left(\frac{R_D}{2}\right)^2} = R_D + m\left(\frac{\lambda}{2}\right) \tag{20}$$

Solving for $R_D$ gives

$$R_D = \frac{4h^2 - \frac{m^2\lambda^2}{4}}{m\lambda} \tag{21}$$

Table 11 shows the distance at which the superpositioned signals result in maximum destructive interference for $h$ = 0.59055 m and wavelength λ at the lower (2.402 GHz), middle (2.441 GHz), and upper end (2.480 GHz) of the Bluetooth frequency band. It is clear that destructive interference occurs when the transmitter and receiver are separated by 3 m or 6 m, each of which correspond to even numbered wavelength intervals. The proximity of the experimental transmitter and receiver separations to these distances is sufficient to explain the drop in RSSI values. The exact power drop is not calculated since the goal of this analytical model was to only explain a probable cause.

### 4.4 Throughput Ranges

The final experiment incorporated the previously determined better receiver orientations to identify some best-case ranges for throughput of Bluetooth transmission. Best-case refers to the best value measured during each experiment rather than the best possible. The hardware consisted of an Anycom Bluetooth CF Card as the transmitter

and an Armadillo Bluetooth CF Card as the receiver, both operating on Dell Inspiron 8200s under Windows 2000. Both Bluetooth cards use the same Ericsson chipset and microstrip patch antenna (c.f., Figure 17).

**Table 11. Destructive Interference Distances**

| Half Wavelengths | Frequency Range: Low | Mid | High | Distance (meters) |
|---|---|---|---|---|
| 1 | 12.63 | 12.84 | 13.05 | |
| 2 | 6.27 | 6.37 | 6.48 | |
| 3 | 4.12 | 4.20 | 4.27 | |
| 4 | 3.04 | 3.10 | 3.15 | |
| 5 | 2.37 | 2.42 | 2.46 | |
| 6 | 1.92 | 1.96 | 2.00 | |
| 7 | 1.59 | 1.62 | 1.66 | |
| 8 | 1.33 | 1.36 | 1.39 | |
| 9 | 1.12 | 1.15 | 1.18 | |
| 10 | 0.95 | 0.98 | 1.01 | |
| 11 | 0.80 | 0.83 | 0.86 | |
| 12 | 0.68 | 0.70 | 0.73 | |
| 13 | 0.56 | 0.59 | 0.61 | |
| 14 | 0.46 | 0.49 | 0.51 | |
| 15 | 0.37 | 0.40 | 0.42 | |
| 16 | 0.29 | 0.31 | 0.33 | |
| 17 | 0.21 | 0.24 | 0.26 | |
| 18 | 0.14 | 0.16 | 0.18 | |
| 19 | 0.07 | 0.09 | 0.11 | |
| 20 | 0.01 | 0.03 | 0.05 | |
| 21 | -0.05 | -0.03 | -0.01 | |
| 22 | -0.11 | -0.09 | -0.07 | |

A Merlin Bluetooth packet analyzer is used to determine the exact time between the first and last DM5 packets. Specific settings for the Merlin are documented in Appendix B. The Merlin actively synchronizes to the master and slave in the piconet and sniffs all traffic on the piconet. Each packet is time stamped at the time of reception. Once the Merlin is synchronized to the piconet it becomes passive and does not transmit. Thus, if a packet is received with errors, the Merlin does not request retransmission. To determine if retransmissions occur due to errors received by the slave, all captured

packets must be carefully analyzed and correlated. This particular task is extremely difficult due to the packet transmission timing and the system storage capabilities. Therefore, throughput calculations by the Merlin do not reflect the true piconet payload throughput. Only the timestamp of when the packet is received is trustworthy. The difference between the first and last DM5 packet timestamps provides the total transmission time of the FTP transaction.

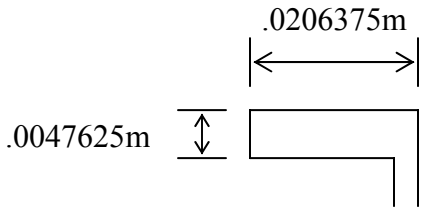


**Figure 17. Microstrip Patch Antenna Dimensions**

The transmitter and receiver are both placed on wooden stools at a height of 0.631825 m. Wooden stools are used to minimize the possibility of interference caused by metal. The receiver orientation is a constant 270-degrees based on the orientation findings of the RSSI experiments and on the likelihood of how a typical receiver is positioned when using a laptop (i.e., person at the keyboard facing the transmitter). The transmitter orientation is varied in 90-degree increments to emulate moving the receiver in a circular pattern around the transmitter at 90-degree increments. Table 12 displays the best-case throughput values measured. Throughput was sampled at 5 m increments and then refined to 1 m increments to determine each of the following throughput level's (300, 200, and 100 kbps) range. A blank entry in the table indicates no values were measured at that distance and orientation. A "fail" entry indicates a distance and orientation at which a connection could not be established or maintained long enough to transfer the file.

**Table 12. FTP Throughput Values (kbps)**

| Distance (meters) | Antenna Orientation (degrees) | | | |
|---|---|---|---|---|
| | 90 | 180 | 270 | 360 |
| 1 | 302.05 | 307.18 | 305.17 | 302.71 |
| 2 | 79.44 | | | |
| 3 | 184.79 | | | |
| 4 | 259.00 | | | |
| 5 | 235.57 | 299.42 | 304.32 | 304.49 |
| 6 | 158.15 | | | |
| 7 | Fail | | | |
| 8 | Fail | | | |
| 9 | Fail | | | |
| 10 | Fail | 221.68 | 300.75 | 302.49 |
| 11 | | | | |
| 12 | | | | |
| 13 | | | | |
| 14 | | | | |
| 15 | | 219.06 | 300.19 | 303.32 |
| 16 | | 173.38 | 224.30 | |
| 17 | | 211.81 | | |
| 18 | | 79.12 | | |
| 19 | | 177.54 | | |
| 20 | | 135.44 | 258.52 | 302.78 |
| 21 | | 106.83 | 225.24 | |
| 22 | | Fail | 187.68 | |
| 23 | | Fail | 138.87 | |
| 24 | | | 140.75 | |
| 25 | | | Fail | 285.25 |
| 26 | | | Fail | 288.01 |
| 27 | | | | 270.56 |
| 28 | | | | 212.42 |
| 29 | | | | 189.86 |
| 30 | | | | 201.75 |
| 31 | | | | 132.97 |
| 32 | | | | 102.75 |
| 33 | | | | 80.10 |
| 34 | | | | 18.55 |
| 35 | | | | 20.44 |

Although it is expected that the best orientation occurs when the transmitter and receiver antennas are set at the 90-degree or 270-degree orientation, based on the outcome of the RSSI tests, the best results are clearly obtained from the 360-degree orientation. Even though this appears contradictory to findings from the antenna

orientation experiments, it is easily explained by considering the asymmetric antenna gain characteristics. Figure 18 shows a comparison between total antenna gain factors, $G_{ij}$, for the orientation and throughput experiments. The 270-degree receiver orientation in the orientation experiment has a total gain factor of $G_{12}$, where $i = 1$ is the transmitter gain and $j = 2$ is the receiver gain. The 360-degree transmitter orientation gain in the throughput experiment is $G_{21}$, where $i = 2$ is the receiver gain and $j = 1$ is the transmitter gain. This shows that the total gain factor in the best-case orientation experiment is the same gain factor producing best results in the throughput experiment ($G_{12} = G_{21}$).

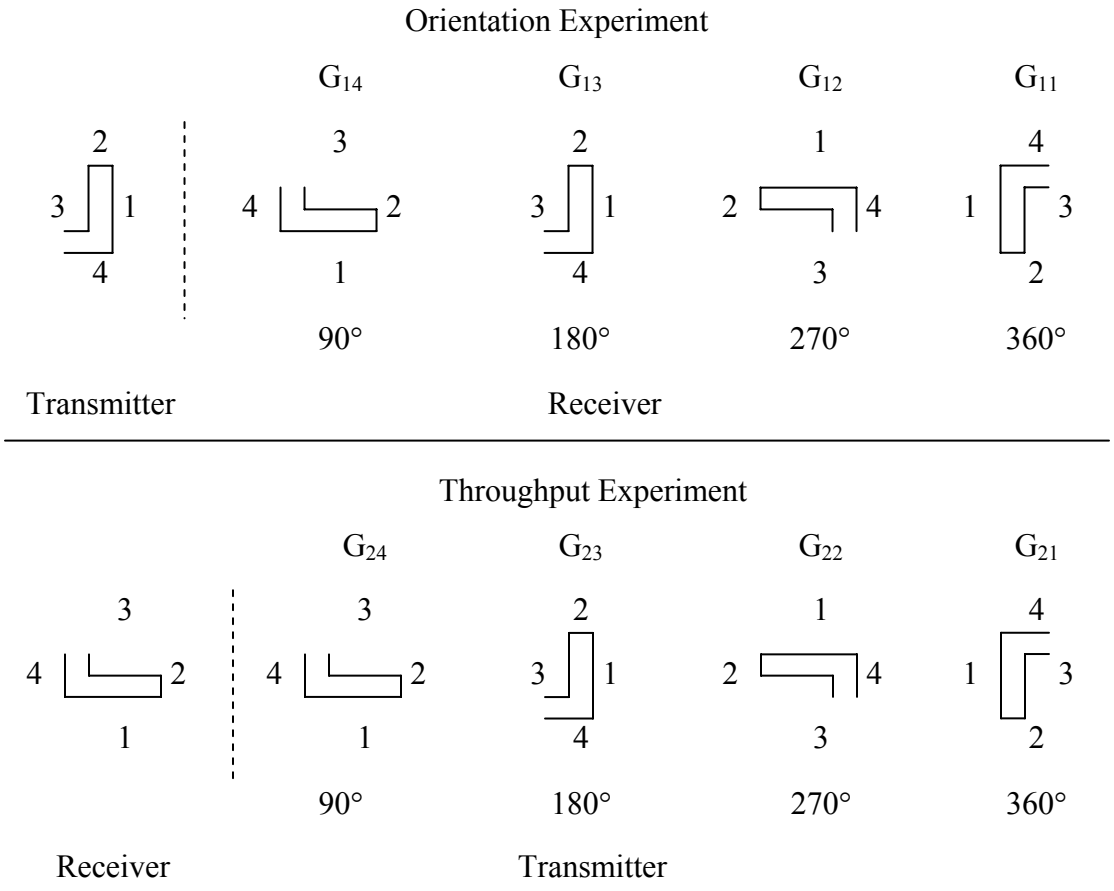


**Figure 18. Total Antenna Gain Factor ($G_{ij}$) Comparison**

Figure 19 shows a mapping of the ranges at which throughput levels of 300 kbps, 200 kbps, and 100 kbps or better were obtained. Although this is a best-case sample, the mapping reflects a more realistic measure of the functional ranges of Bluetooth devices. The devices are required to operate with a raw bit error rate (BER) of $10^{-3}$ when receiving a signal of –70 dBm or better. Additionally, the 20 dB width of the Golden Receive Range crudely equates to a physical factor of ten. Thus, when a signal is received within 10 m, it should be in the Golden Range and the throughput at its maximum. Outside 10 m, the signal strength decreases as the distance increases. The throughput level is maintained until minimum signal strength of –70 dBm is reached. The 10 m functional range of Bluetooth, as defined in the specification, is a minimum standard for manufacturer compliance. It is clear that the functional range for the devices tested is well beyond the 10 m minimum and that a throughput level equivalent to best sampled is achievable at over twice the 10 m minimum.

As shown in Table 12, a throughput level of approximately 300 kbps is achievable at a distance of 20 m. This level of throughput is equivalent to that achieved within the 10 m functional range. Comparing this distance to the RSSI values sampled shows that the RSSI values for any given orientation at this range had reached the lower bound established by the manufacturer. Thus, it is not possible to correlate the RSSI values and throughput.

## 4.5 Summary

This chapter discussed the orientation and throughput experiments performed, the data collected, and analysis. Additionally, a signal interference model was developed to explain anomalies in the sampled RSSI values. The orientation experiment showed that

certain orientations of the Bluetooth device antenna received stronger signals than others and that the orientation of the antenna is a statistically significant factor.

The signal interference model showed the ranges at which destructive interference of the Bluetooth transmissions occur. This accounted for the dips in the RSSI values. The throughput experiment developed a 360-degree mapping of throughput ranges for a single configuration of the transmitter antenna. The next chapter discusses this study as a whole and the conclusions drawn from it.

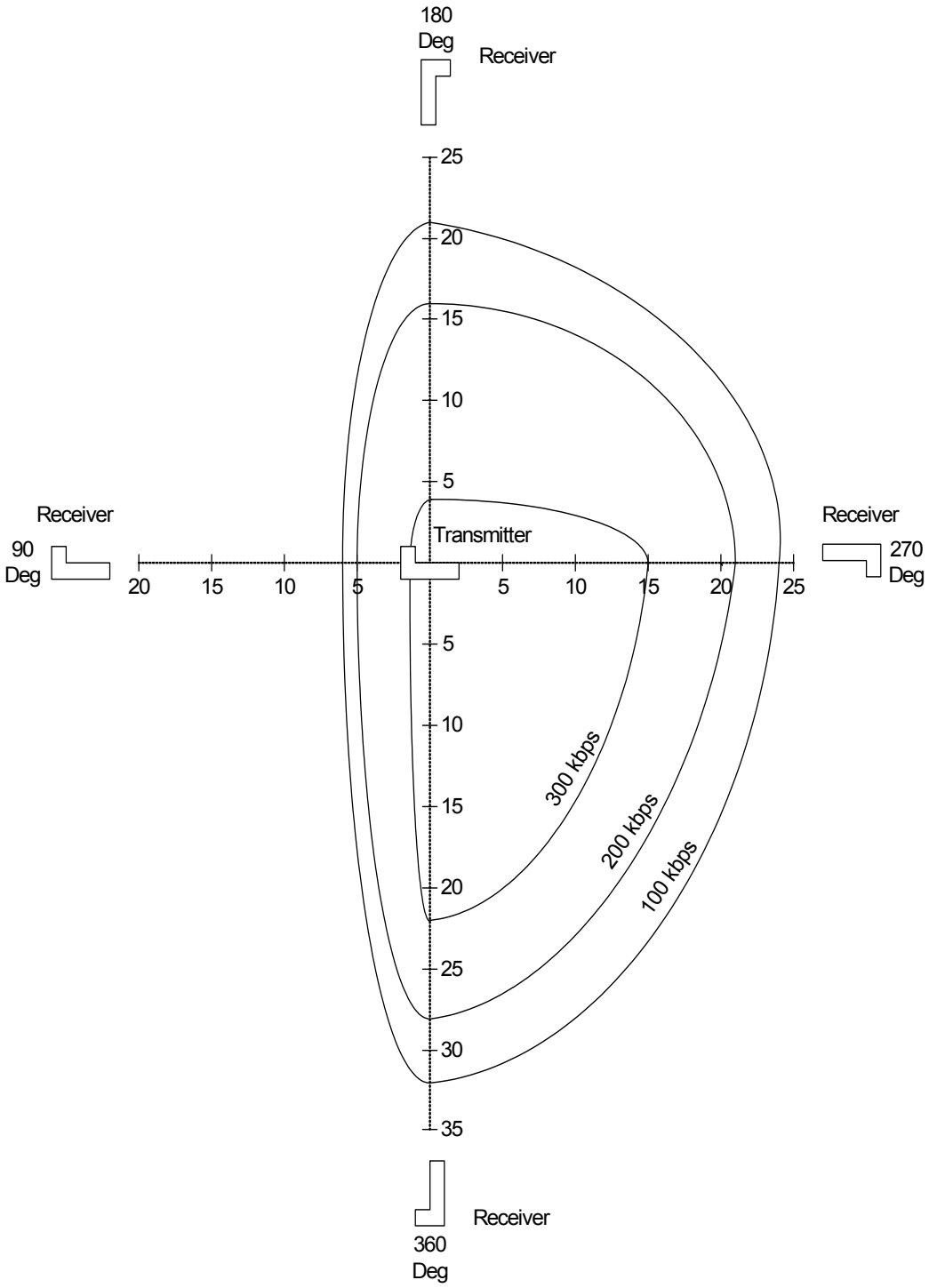


**Figure 19. Throughput Ranges (meters)**

# *5. Conclusions*

## 5.1 Introduction

This chapter reviews and summarizes the research and the research objectives. First, the impact of the research is discussed and its implications for using Bluetooth devices within the DoD. Next, objectives and their respective experiments are reviewed along with conclusions drawn. Last, potential follow on areas of study are outlined.

## 5.2 Research Impact

The security risks associated with the interception of Bluetooth communications drove the research objectives. The first objective, identification of the best antenna orientation for a common use configuration is incorporated into the experiment to support the second objective. The second objective, determining throughput ranges, is used to identify the zones of vulnerability for interception. Together, the objectives of this study define an approximate distance needed to intercept Bluetooth transmissions.

### 5.2.1 Orientation

The orientation of the micro-strip patch antenna of a Bluetooth device is a significant factor in achieving a certain throughput threshold. In the experiments conducted, antenna orientation accounted for approximately 14% of the variance in recorded RSSI values. This means that antenna orientation must be taken into account when determining the throughput ranges of a Bluetooth device. Thus, throughput experiments must include antenna orientation as a factor rather than measuring throughput at distances varied along a single linear path. Additionally, this indicates that different levels of throughput can be expected for different orientations.

Transmitter/receiver distance contributed nearly 78% to the variance in RSSI values. This validated the expectation that path loss is a primary cause for drop in signal strength. An interesting anomaly was identified during the course of the orientation experiments. Destructive interference caused by reflected signal induced fluctuations in signal strength as the distance between the transmitter and receiver varied. This implies that signal strength cannot be expected to monotonically decrease due to path loss, but will fluctuate. This fluctuation could impact throughput levels as well, but this was not validated in this thesis.

### 5.2.2 Ranges of Throughput

Different throughput levels were measured for each orientation and distance on a best-case basis. Throughput levels fluctuated slightly as predicted, but dropped off consistently once a certain distance was reached. The distance of a given throughput level varied from orientation to orientation as expected. The best throughput levels were achieved using a transmitter orientation of 360-degrees. This appeared to contradict the expected best orientation of 90-degrees or 270-degrees. This deviation is explained by comparing the antenna gain patterns of the two experiments and showing that the gain patterns of the 270-degree orientation in the orientation experiment was the same gain pattern as the 360-degree orientation in the throughput experiment.

The throughput levels were categorized based on the last distance at which a given level or better was achieved. From this, a 360-degree mapping was produced to graphically reflect the potential zones of vulnerability. Although only four orientations were used to generate the map, the arcs between the 90-degree orientation increments show the expected throughput ranges when transitioning between one orientation and the

next. This mapping reflects the best-case throughput levels achieved and shows that the primary zone of vulnerability is between the 270-degree and 360-degree transmitter orientations.

The throughput level achieved for the 360-degree transmitter orientation was equivalent to that achieved when the signal strength was within the Golden Receive Range at twice the 10 m minimum distance defined by the core specification. Comparing this distance to the distances at which the RSSI values were measured, it was seen that the RSSI values reach their lower bound at approximately the same distance. Thus, no correlation can be drawn between the RSSI value and the level of throughput for the configuration used since no change in throughput is observed within the range that the RSSI can be measured.

## 5.3 Outlines of Future Work

This thesis provides a preliminary look at the orientation of a Bluetooth device antenna and a mapping of throughput ranges for a specific device configuration. This is only an initial look and provides a foundation for areas of further research. Some future areas of research include:

- Refined measurement of throughput levels for different packet types and transmitter orientations
- Throughput level mapping for different device antennas, both modified and unmodified
- Passive determination of frequency hopping sequence of a piconet
- Passive synchronization to frequency hopping sequence of a piconet
- Correlation of signal interference model to throughput level fluctuation
- Passive identification of devices in a piconet

## 5.4 Summary

This research determined the effects of antenna orientation on signal strength for Bluetooth devices as well as developed a mapping of ranges of different throughput levels for a specific Bluetooth device configuration. The antenna orientation experiments determined the significance of antenna orientation on throughput ranges. Additionally, a basic signal interference model was introduced to explain fluctuations in signal strength. The throughput experiment generated a mapping of set levels of throughput for certain distances and orientations. The mapping depicts zones of vulnerability for Bluetooth communication interception. Together, these provide a first look study of Bluetooth communications and provide ideas for further future studies.

## *Appendix A. Receiver Signal Strength Indicator Linux Script*

```
# RSSI Sampler by Tim Kneeland
# Last updated Dec 2, 2002
# This script samples Receiver Signal Strength Indicator values and outputs
# them to a file.  A connection must be established first with a transmitter
# using "hcitool cc <BD_ADDR>".  Script execution requires three command line
# arguments following script name. First argument is the BD_ADDR of the
# transmitter a connection is established with.  Second argument is the name
# of the output file to append the data too.  Third argument is the number of
# RSSI samples to take for each orientation and distance measurement.  Script
# will prompt for distance in meters (integer values only) and prompt to change
# orientation of receiver.  Script is exited by input of a distance of 99.

# Output the date to file
# date >> $2
# A distance of 99 will exit the script
distance=0
while [ $distance -le 99 ]
do
 # Prompt for distance
 echo -n "Input distance between transmitter and receiver in meters: "
 read distance
 if [ $distance -eq 99 ]
 then
  exit 1
 fi
 # Output distance to file
 echo "Distance in meters: $distance" >> $2
 # Four different orientations
 for iteration in 1 2 3 4
 do
  # Prompt for proper orientation of receiver
  echo -n "Place receiver at `expr 90 \* $iteration` degrees and hit enter."
  read z
  echo "" >> $2
  echo "Orientation in degrees: `expr 90 \* $iteration`" >> $2
  # Sample RSSI the number of times specified by the third argument
  x=1
  while [ $x -le $3 ]
  do
        hcitool rssi $1 >> $2
        x=`expr $x + 1`
  done
 done
done
```

## *Appendix B. Merlin Bluetooth Packet Analyzer Settings for Throughput Experiments*

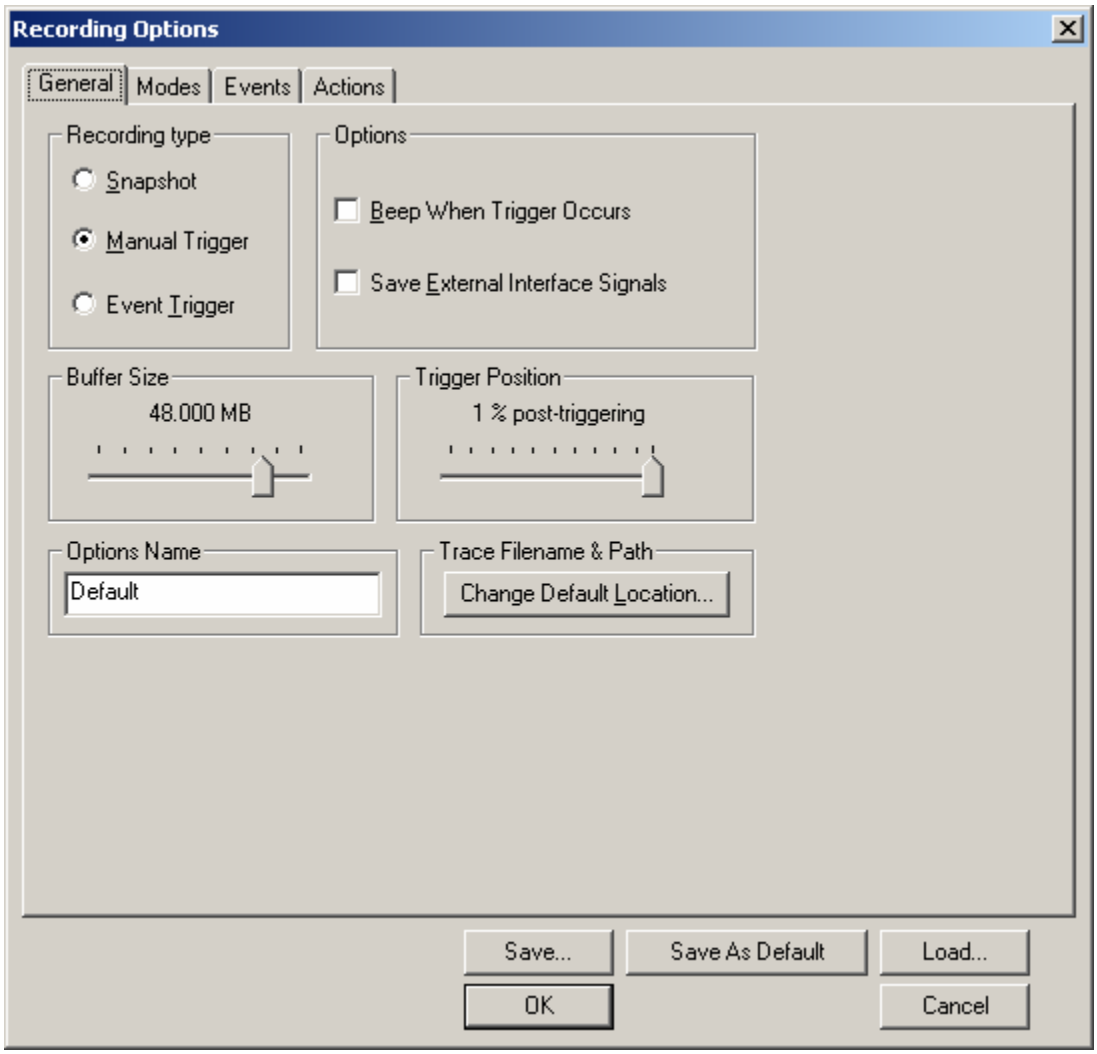


**Figure 20. Merlin General Recording Options**

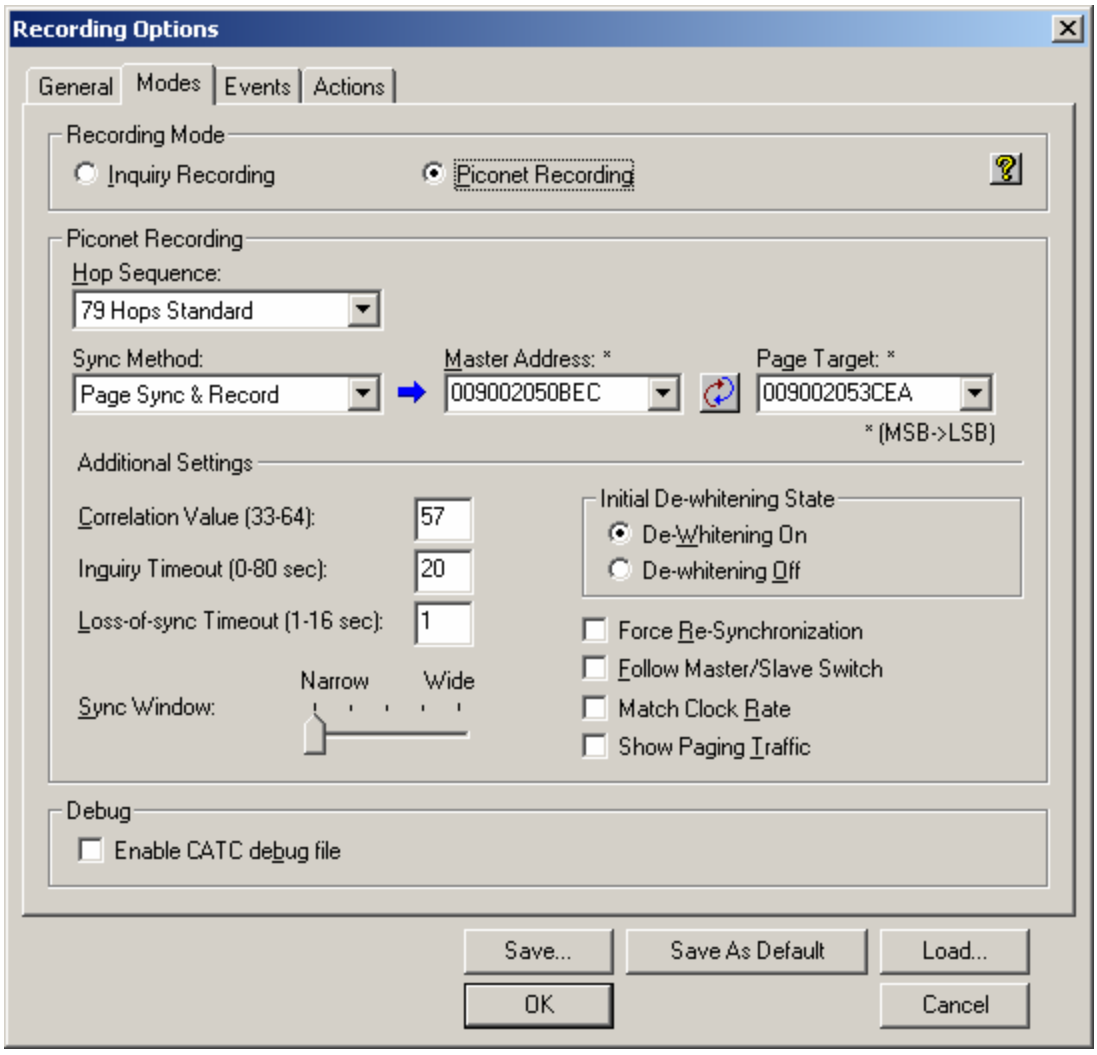


**Figure 21. Merlin Modes Recording Options**

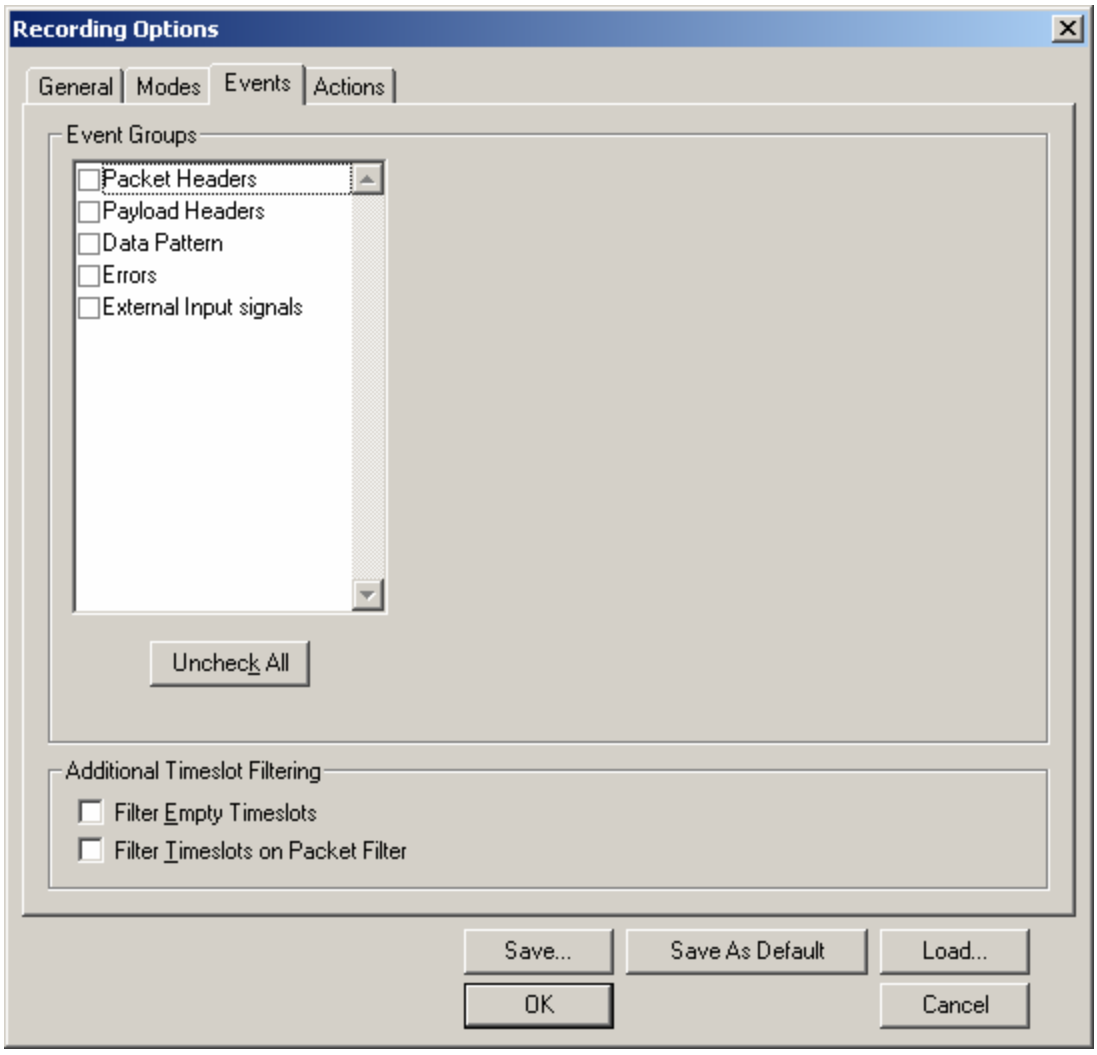


**Figure 22. Merlin Events Recording Options**

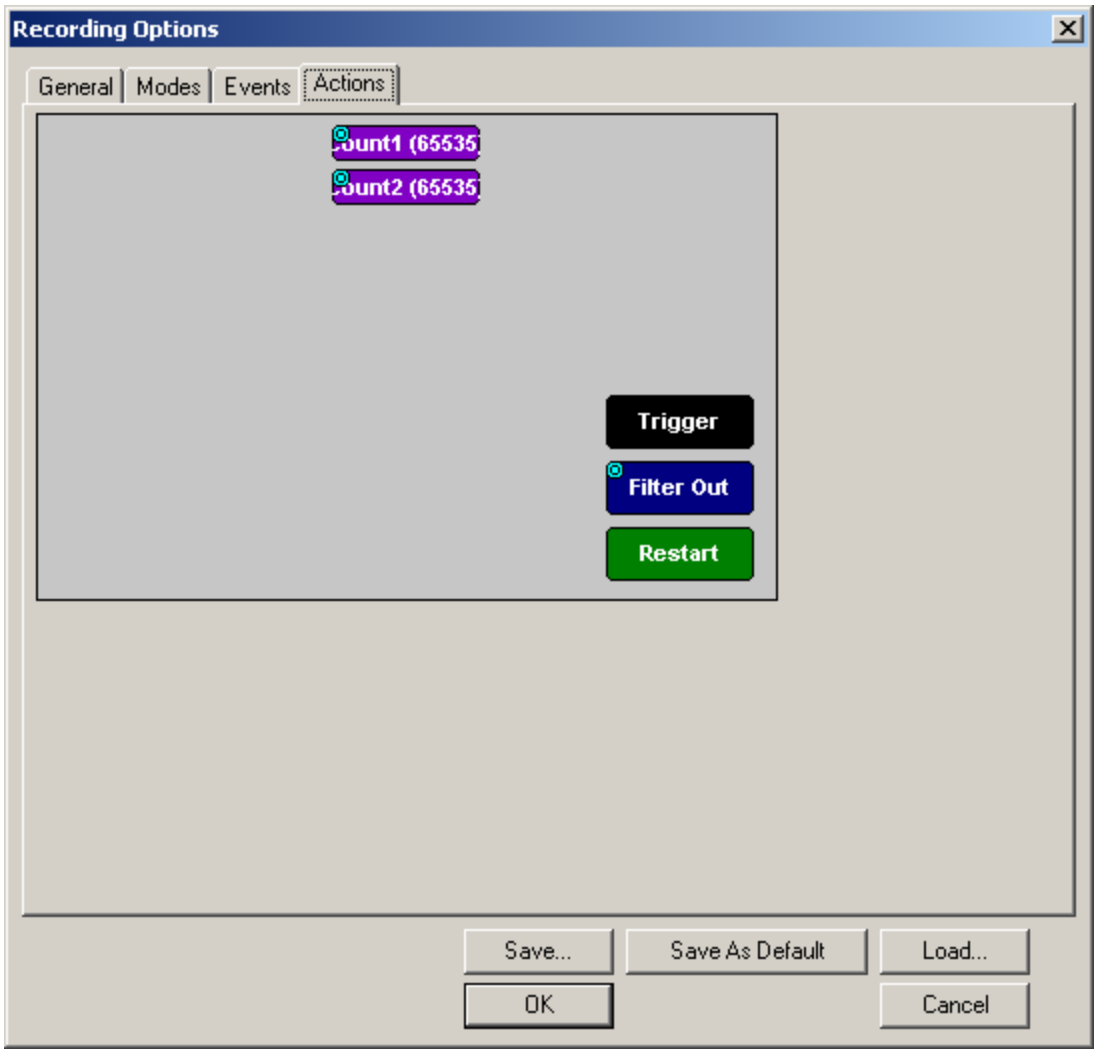


**Figure 23. Merlin Actions Recording Options**

## *Appendix C. Experiment Data Analysis Tables*

**Table 13. Computation of Effects for Experiment 1**

| | | Orientation | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | 90 | 180 | 270 | 360 | Row Sum | Row Mean | Row Effect |
| Distance | 1 | 0.00 | -2.66 | 0.00 | -3.34 | -6.00 | -1.50 | 10.22 |
| | 2 | 0.00 | -5.00 | 0.00 | -8.04 | -13.04 | -3.26 | 8.46 |
| | 3 | -5.43 | -8.50 | -5.81 | -12.74 | -32.48 | -8.12 | 3.60 |
| | 4 | -4.26 | -9.77 | -4.70 | -12.84 | -31.57 | -7.89 | 3.82 |
| | 5 | -6.98 | -13.36 | -11.38 | -13.56 | -45.28 | -11.32 | 0.40 |
| | 6 | -12.87 | -13.12 | -12.96 | -13.80 | -52.75 | -13.19 | -1.47 |
| | 7 | -13.22 | -11.90 | -12.52 | -15.00 | -52.64 | -13.16 | -1.44 |
| | 8 | -10.13 | -13.00 | -10.15 | -13.92 | -47.20 | -11.80 | -0.08 |
| | 9 | -10.30 | -12.80 | -10.70 | -15.00 | -48.80 | -12.20 | -0.48 |
| | 10 | -9.76 | -12.56 | -10.06 | -15.00 | -47.38 | -11.85 | -0.13 |
| | 11 | -10.79 | -13.24 | -10.85 | -15.00 | -49.88 | -12.47 | -0.75 |
| | 12 | -10.65 | -15.00 | -10.00 | -15.00 | -50.65 | -12.66 | -0.95 |
| | 13 | -11.06 | -14.08 | -11.13 | -15.00 | -51.27 | -12.82 | -1.10 |
| | 14 | -12.04 | -14.88 | -11.36 | -15.00 | -53.28 | -13.32 | -1.60 |
| | 15 | -12.16 | -14.80 | -12.10 | -15.00 | -54.06 | -13.52 | -1.80 |
| | 16 | -13.16 | -14.68 | -13.12 | -15.00 | -55.96 | -13.99 | -2.27 |
| | 17 | -14.46 | -15.00 | -13.00 | -15.00 | -57.46 | -14.37 | -2.65 |
| | 18 | -13.44 | -15.00 | -13.00 | -15.00 | -56.44 | -14.11 | -2.39 |
| | 19 | -13.38 | -15.00 | -14.78 | -15.00 | -58.16 | -14.54 | -2.82 |
| | 20 | -15.00 | -15.00 | -14.94 | -15.00 | -59.94 | -14.99 | -3.27 |
| | 21 | -15.00 | -15.00 | -15.00 | -15.00 | -60.00 | -15.00 | -3.28 |
| | Column Sum | -214.09 | -264.35 | -217.56 | -288.24 | -984.24 | | |
| | Column Mean | -10.19 | -12.59 | -10.36 | -13.73 | | -11.72 | |
| | Column Effect | 1.52 | -0.87 | 1.36 | -2.01 | | | |

**Table 14. Error Computation for Experiment 1**

| | | Orientation | | | |
|---|---|---|---|---|---|
| | | 90 | 180 | 270 | 360 |
| Distance | 1 | -0.02 | -0.29 | 0.14 | 0.17 |
| | 2 | 1.74 | -0.87 | 1.90 | -2.77 |
| | 3 | 1.17 | 0.49 | 0.95 | -2.61 |
| | 4 | 2.11 | -1.01 | 1.84 | -2.94 |
| | 5 | 2.82 | -1.17 | -1.42 | -0.23 |
| | 6 | -1.20 | 0.94 | -1.13 | 1.40 |
| | 7 | -1.58 | 2.13 | -0.72 | 0.17 |
| | 8 | 0.15 | -0.33 | 0.29 | -0.11 |
| | 9 | 0.38 | 0.27 | 0.14 | -0.79 |
| | 10 | 0.56 | 0.16 | 0.43 | -1.15 |
| | 11 | 0.16 | 0.10 | 0.26 | -0.52 |
| | 12 | 0.49 | -1.47 | 1.31 | -0.33 |
| | 13 | 0.24 | -0.39 | 0.33 | -0.17 |
| | 14 | -0.24 | -0.69 | 0.60 | 0.33 |
| | 15 | -0.17 | -0.41 | 0.06 | 0.52 |
| | 16 | -0.69 | 0.18 | -0.49 | 1.00 |
| | 17 | -1.62 | 0.24 | 0.01 | 1.37 |
| | 18 | -0.85 | -0.02 | -0.25 | 1.12 |
| | 19 | -0.36 | 0.41 | -1.60 | 1.55 |
| | 20 | -1.54 | 0.86 | -1.31 | 1.99 |
| | 21 | -1.52 | 0.87 | -1.36 | 2.01 |

**Table 15. Error Squares for Experiment 1**

| | | Orientation | | | | |
|---|---|---|---|---|---|---|
| | | 90 | 180 | 270 | 360 | |
| Distance | 1 | 0.00 | 0.08 | 0.02 | 0.03 | 0.13 |
| | 2 | 3.02 | 0.76 | 3.62 | 7.68 | 15.08 |
| | 3 | 1.36 | 0.24 | 0.91 | 6.82 | 9.33 |
| | 4 | 4.45 | 1.01 | 3.37 | 8.64 | 17.47 |
| | 5 | 7.94 | 1.37 | 2.01 | 0.05 | 11.37 |
| | 6 | 1.45 | 0.88 | 1.28 | 1.95 | 5.56 |
| | 7 | 2.50 | 4.54 | 0.51 | 0.03 | 7.59 |
| | 8 | 0.02 | 0.11 | 0.09 | 0.01 | 0.23 |
| | 9 | 0.14 | 0.07 | 0.02 | 0.63 | 0.86 |
| | 10 | 0.32 | 0.02 | 0.18 | 1.31 | 1.84 |
| | 11 | 0.02 | 0.01 | 0.07 | 0.27 | 0.38 |
| | 12 | 0.24 | 2.15 | 1.70 | 0.11 | 4.20 |
| | 13 | 0.06 | 0.15 | 0.11 | 0.03 | 0.35 |
| | 14 | 0.06 | 0.47 | 0.36 | 0.11 | 1.00 |
| | 15 | 0.03 | 0.17 | 0.00 | 0.27 | 0.48 |
| | 16 | 0.48 | 0.03 | 0.24 | 1.00 | 1.75 |
| | 17 | 2.62 | 0.06 | 0.00 | 1.89 | 4.56 |
| | 18 | 0.73 | 0.00 | 0.06 | 1.25 | 2.04 |
| | 19 | 0.13 | 0.17 | 2.55 | 2.40 | 5.25 |
| | 20 | 2.36 | 0.73 | 1.72 | 3.97 | 8.79 |
| | 21 | 2.32 | 0.76 | 1.84 | 4.03 | 8.95 |

**Table 16. Sample Squares for Experiment 1**

| | | Orientation | | | | |
|---|---|---|---|---|---|---|
| | | 90 | 180 | 270 | 360 | Row Sum |
| Distance | 1 | 0.00 | 7.07 | 0.00 | 11.15 | 18.23 |
| | 2 | 0.00 | 25.00 | 0.00 | 64.64 | 89.64 |
| | 3 | 29.48 | 72.25 | 33.75 | 162.30 | 297.79 |
| | 4 | 18.14 | 95.45 | 22.09 | 164.86 | 300.55 |
| | 5 | 48.72 | 178.48 | 129.50 | 183.87 | 540.58 |
| | 6 | 165.63 | 172.13 | 167.96 | 190.44 | 696.17 |
| | 7 | 174.76 | 141.61 | 156.75 | 225.00 | 698.12 |
| | 8 | 102.61 | 169.00 | 103.02 | 193.76 | 568.40 |
| | 9 | 106.09 | 163.84 | 114.49 | 225.00 | 609.42 |
| | 10 | 95.25 | 157.75 | 101.20 | 225.00 | 579.21 |
| | 11 | 116.42 | 175.29 | 117.72 | 225.00 | 634.44 |
| | 12 | 113.42 | 225.00 | 100.00 | 225.00 | 663.42 |
| | 13 | 122.32 | 198.24 | 123.87 | 225.00 | 669.44 |
| | 14 | 144.96 | 221.41 | 129.04 | 225.00 | 720.42 |
| | 15 | 147.86 | 219.04 | 146.41 | 225.00 | 738.31 |
| | 16 | 173.18 | 215.50 | 172.13 | 225.00 | 785.82 |
| | 17 | 209.09 | 225.00 | 169.00 | 225.00 | 828.09 |
| | 18 | 180.63 | 225.00 | 169.00 | 225.00 | 799.63 |
| | 19 | 179.02 | 225.00 | 218.44 | 225.00 | 847.47 |
| | 20 | 225.00 | 225.00 | 223.20 | 225.00 | 898.20 |
| | 21 | 225.00 | 225.00 | 225 | 225.00 | 900 |
| | Column Sum | 2577.65 | 3562.10 | 2622.62 | 4121.05 | |
| | | | | | SSY = | 12883.44 |
| | | | | | SS0 = | 11532.48 |
| | | | | | SSA = | 188.00 |
| | | | | | SSB = | 1049.91 |
| | | | | | SSAB = | 107.20 |
| | | | | | SST = | 1350.96 |
| | | | | | SSE = | 5.84 |
| | | | | | Explained by Orientation = | 13.92% |
| | | | | | Explained by Distance = | 77.72% |
| | | | | | Explained by Interactions = | 7.94% |
| | | | | | Unexplained = | 0.43% |

**Table 17. ANOVA for Experiment 1**

| Component | Sum of Squares | Percentage of Variation | Degrees of Freedom | Mean Square | F-Computed | F-Table 99% |
|---|---|---|---|---|---|---|
| y | 12883.44 | | 84 | | | |
| y.. | 11532.48 | | 1 | | | |
| y-y.. | 1350.96 | 100.00% | 83 | | | |
| Orientation | 188.00 | 13.92% | 3 | 62.67 | 643.62 | 4.31 |
| Distance | 1049.91 | 77.72% | 20 | 52.50 | 539.16 | 2.37 |
| Errors | 5.84 | 0.43% | 60 | 0.10 | | |

| | |
|---|---|
| Std Dev Errors = | 0.31 |
| Std Dev Mean = | 0.03 |
| Std Dev Orientation = | 0.06 |
| Std Dev Distance = | 0.15 |

**Table 18. 90% Confidence Intervals for Effects for Experiment 1**

| Parameter | Mean Effect | Std Dev | Conf Interval | |
|---|---|---|---|---|
| Mean | -984.24 | 0.03 | -984.30 | -984.18 |
| Orientation | | | | |
| 90 | 1.52 | 0.06 | 1.42 | 1.62 |
| 180 | -0.87 | 0.06 | -0.97 | -0.77 |
| 270 | 1.36 | 0.06 | 1.26 | 1.46 |
| 360 | -2.01 | 0.06 | -2.11 | -1.91 |
| Distance | | | | |
| 1 | 10.22 | 0.15 | 9.96 | 10.47 |
| 2 | 8.46 | 0.15 | 8.20 | 8.71 |
| 3 | 3.60 | 0.15 | 3.34 | 3.85 |
| 4 | 3.82 | 0.15 | 3.57 | 4.08 |
| 5 | 0.40 | 0.15 | 0.14 | 0.65 |
| 6 | -1.47 | 0.15 | -1.72 | -1.22 |
| 7 | -1.44 | 0.15 | -1.70 | -1.19 |
| 8 | -0.08 | 0.15 | -0.34 | 0.17 |
| 9 | -0.48 | 0.15 | -0.74 | -0.23 |
| 10 | -0.13 | 0.15 | -0.38 | 0.13 |
| 11 | -0.75 | 0.15 | -1.01 | -0.50 |
| 12 | -0.95 | 0.15 | -1.20 | -0.69 |
| 13 | -1.10 | 0.15 | -1.35 | -0.85 |
| 14 | -1.60 | 0.15 | -1.86 | -1.35 |
| 15 | -1.80 | 0.15 | -2.05 | -1.54 |
| 16 | -2.27 | 0.15 | -2.53 | -2.02 |
| 17 | -2.65 | 0.15 | -2.90 | -2.39 |
| 18 | -2.39 | 0.15 | -2.65 | -2.14 |
| 19 | -2.82 | 0.15 | -3.08 | -2.57 |
| 20 | -3.27 | 0.15 | -3.52 | -3.01 |
| 21 | -3.28 | 0.15 | -3.54 | -3.03 |

* Not Significant

**Table 19. Computation of Effects for Experiment 2**

| | | Orientation | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | 90 | 180 | 270 | 360 | Row Sum | Row Mean | Row Effect |
| Distance | 1 | 0.00 | -2.66 | 0.00 | -3.34 | -6.00 | -1.50 | 10.21 |
| | 2 | 0.00 | -5.00 | 0.00 | -8.04 | -13.04 | -3.26 | 8.45 |
| | 3 | -4.72 | -8.25 | -5.02 | -11.01 | -29.01 | -7.25 | 4.46 |
| | 4 | -4.93 | -11.93 | -3.08 | -11.97 | -31.92 | -7.98 | 3.73 |
| | 5 | -11.69 | -15.00 | -10.64 | -13.01 | -50.35 | -12.59 | -0.88 |
| | 6 | -14.02 | -13.00 | -12.99 | -14.98 | -54.99 | -13.75 | -2.04 |
| | 7 | -12.26 | -12.81 | -10.03 | -15.00 | -50.11 | -12.53 | -0.82 |
| | 8 | -9.96 | -12.97 | -9.94 | -15.00 | -47.88 | -11.97 | -0.26 |
| | 9 | -10.00 | -12.96 | -10.00 | -15.00 | -47.96 | -11.99 | -0.28 |
| | 10 | -9.76 | -13.00 | -8.43 | -15.00 | -46.19 | -11.55 | 0.16 |
| | 11 | -9.83 | -13.24 | -10.85 | -15.00 | -48.92 | -12.23 | -0.52 |
| | 12 | -10.65 | -15.00 | -10.00 | -15.00 | -50.65 | -12.66 | -0.95 |
| | 13 | -11.06 | -14.08 | -11.13 | -15.00 | -51.27 | -12.82 | -1.11 |
| | 14 | -12.04 | -14.88 | -11.36 | -15.00 | -53.28 | -13.32 | -1.61 |
| | 15 | -12.16 | -14.80 | -12.10 | -15.00 | -54.06 | -13.52 | -1.81 |
| | 16 | -13.16 | -14.68 | -13.12 | -15.00 | -55.96 | -13.99 | -2.28 |
| | 17 | -14.46 | -15.00 | -13.00 | -15.00 | -57.46 | -14.37 | -2.66 |
| | 18 | -13.44 | -15.00 | -13.00 | -15.00 | -56.44 | -14.11 | -2.40 |
| | 19 | -13.38 | -15.00 | -14.78 | -15.00 | -58.16 | -14.54 | -2.83 |
| | 20 | -15.00 | -15.00 | -14.94 | -15.00 | -59.94 | -14.99 | -3.28 |
| | 21 | -15.00 | -15.00 | -15.00 | -15.00 | -60.00 | -15.00 | -3.29 |
| | Column Sum | -217.55 | -269.27 | -209.44 | -287.35 | -983.61 | | |
| | Column Mean | -10.36 | -12.82 | -9.97 | -13.68 | | -11.71 | |
| | Column Effect | 1.35 | -1.11 | 1.74 | -1.97 | | | |

**Table 20. Error Computation for Experiment 2**

| | | Orientation | | | |
|---|---|---|---|---|---|
| | | 90 | 180 | 270 | 360 |
| Distance | 1 | 0.15 | -0.05 | -0.24 | 0.13 |
| | 2 | 1.91 | -0.63 | 1.52 | -2.81 |
| | 3 | 1.18 | 0.11 | 0.49 | -1.78 |
| | 4 | 1.69 | -2.84 | 3.16 | -2.01 |
| | 5 | -0.46 | -1.30 | 0.21 | 1.55 |
| | 6 | -1.62 | 1.86 | -0.98 | 0.74 |
| | 7 | -1.09 | 0.83 | 0.76 | -0.50 |
| | 8 | 0.66 | 0.11 | 0.29 | -1.06 |
| | 9 | 0.64 | 0.14 | 0.26 | -1.04 |
| | 10 | 0.44 | -0.34 | 1.38 | -1.48 |
| | 11 | 1.04 | 0.10 | -0.35 | -0.79 |
| | 12 | 0.66 | -1.22 | 0.93 | -0.36 |
| | 13 | 0.41 | -0.15 | -0.05 | -0.21 |
| | 14 | -0.07 | -0.45 | 0.22 | 0.29 |
| | 15 | 0.01 | -0.17 | -0.32 | 0.49 |
| | 16 | -0.52 | 0.42 | -0.87 | 0.96 |
| | 17 | -1.44 | 0.48 | -0.37 | 1.34 |
| | 18 | -0.68 | 0.22 | -0.63 | 1.08 |
| | 19 | -0.19 | 0.65 | -1.98 | 1.51 |
| | 20 | -1.36 | 1.10 | -1.69 | 1.96 |
| | 21 | -1.35 | 1.11 | -1.74 | 1.97 |

**Table 21. Error Squares for Experiment 2**

| | | Orientation | | | | |
|---|---|---|---|---|---|---|
| | | 90 | 180 | 270 | 360 | |
| Distance | 1 | 0.02 | 0.00 | 0.06 | 0.02 | 0.10 |
| | 2 | 3.65 | 0.39 | 2.32 | 7.88 | 14.24 |
| | 3 | 1.40 | 0.01 | 0.24 | 3.18 | 4.83 |
| | 4 | 2.87 | 8.07 | 9.98 | 4.05 | 24.98 |
| | 5 | 0.21 | 1.69 | 0.04 | 2.40 | 4.34 |
| | 6 | 2.64 | 3.46 | 0.96 | 0.55 | 7.61 |
| | 7 | 1.19 | 0.69 | 0.58 | 0.25 | 2.70 |
| | 8 | 0.44 | 0.01 | 0.08 | 1.12 | 1.65 |
| | 9 | 0.41 | 0.02 | 0.07 | 1.07 | 1.56 |
| | 10 | 0.19 | 0.11 | 1.90 | 2.18 | 4.39 |
| | 11 | 1.09 | 0.01 | 0.13 | 0.63 | 1.86 |
| | 12 | 0.44 | 1.50 | 0.86 | 0.13 | 2.93 |
| | 13 | 0.17 | 0.02 | 0.00 | 0.04 | 0.23 |
| | 14 | 0.00 | 0.20 | 0.05 | 0.09 | 0.34 |
| | 15 | 0.00 | 0.03 | 0.10 | 0.24 | 0.37 |
| | 16 | 0.27 | 0.18 | 0.75 | 0.93 | 2.13 |
| | 17 | 2.09 | 0.23 | 0.14 | 1.79 | 4.25 |
| | 18 | 0.46 | 0.05 | 0.39 | 1.17 | 2.08 |
| | 19 | 0.04 | 0.43 | 3.91 | 2.29 | 6.66 |
| | 20 | 1.86 | 1.21 | 2.86 | 3.84 | 9.76 |
| | 21 | 1.82 | 1.24 | 3.01 | 3.89 | 9.97 |

**Table 22. Sample Squares for Experiment 2**

| | | Orientation | | | | |
|---|---|---|---|---|---|---|
| | | 90 | 180 | 270 | 360 | Row Sum |
| Distance | 1 | 0.00 | 7.08 | 0.00 | 11.16 | 18.23 |
| | 2 | 0.00 | 25.00 | 0.00 | 64.64 | 89.64 |
| | 3 | 22.28 | 68.11 | 25.28 | 121.20 | 236.87 |
| | 4 | 24.36 | 142.42 | 9.51 | 143.19 | 319.48 |
| | 5 | 136.80 | 225.00 | 113.25 | 169.31 | 644.36 |
| | 6 | 196.62 | 169.00 | 168.79 | 224.40 | 758.81 |
| | 7 | 150.50 | 164.10 | 100.64 | 225.00 | 640.24 |
| | 8 | 99.20 | 168.32 | 98.92 | 225.00 | 591.45 |
| | 9 | 100.08 | 168.01 | 100.00 | 225.00 | 593.09 |
| | 10 | 95.26 | 169.00 | 71.17 | 225.00 | 560.42 |
| | 11 | 96.79 | 175.30 | 117.72 | 225.00 | 614.81 |
| | 12 | 113.42 | 225.00 | 100.00 | 225.00 | 663.42 |
| | 13 | 122.32 | 198.25 | 123.88 | 225.00 | 669.45 |
| | 14 | 144.96 | 221.41 | 129.05 | 225.00 | 720.43 |
| | 15 | 147.87 | 219.04 | 146.41 | 225.00 | 738.32 |
| | 16 | 173.19 | 215.50 | 172.13 | 225.00 | 785.82 |
| | 17 | 209.09 | 225.00 | 169.00 | 225.00 | 828.09 |
| | 18 | 180.63 | 225.00 | 169.00 | 225.00 | 799.63 |
| | 19 | 179.02 | 225.00 | 218.45 | 225.00 | 847.47 |
| | 20 | 225.00 | 225.00 | 223.20 | 225.00 | 898.20 |
| | 21 | 225.00 | 225.00 | 225.00 | 225.00 | 900.00 |
| Column Sum | | 2642.39 | 3685.54 | 2481.41 | 4108.89 | |

| | |
|---|---|
| SSY = | 12918.24 |
| SS0 = | 11517.82 |
| SSA = | 209.38 |
| SSB = | 1079.35 |
| SSAB = | 106.97 |
| SST = | 1400.43 |
| SSE = | 4.72 |

| | |
|---|---|
| Explained by Orientation = | 14.95% |
| Explained by Distance = | 77.07% |
| Explained by Interactions = | 7.64% |
| Unexplained = | 0.34% |

**Table 23. ANOVA for Experiment 2**

| Component | Sum of Squares | Percentage of Variation | Degrees of Freedom | Mean Square | F-Computed | F-Table |
|---|---|---|---|---|---|---|
| y | 12918.24 | | 84 | | | |
| y.. | 11517.82 | | 1 | | | |
| y-y.. | 1400.43 | 100.00% | 83 | | | |
| Orientation | 209.38 | 14.95% | 3 | 69.79 | 886.71 | 4.31 |
| Distance | 1079.35 | 77.07% | 20 | 53.97 | 685.65 | 2.37 |
| Errors | 4.72 | 0.34% | 60 | 0.08 | | |

| | |
|---|---|
| Std Dev Errors = | 0.28 |
| Std Dev Mean = | 0.03 |
| Std Dev Orientation = | 0.05 |
| Std Dev Distance = | 0.14 |

**Table 24. 90% Confidence Intervals for Effects for Experiment 2**

| Parameter | Mean Effect | Std Dev | Conf Interval | |
|---|---|---|---|---|
| Mean | -11.71 | 0.03 | -11.76 | -11.66 |
| Orientation | | | | |
| 90 | 1.35 | 0.05 | 1.26 | 1.44 |
| 180 | -1.11 | 0.05 | -1.20 | -1.02 |
| 270 | 1.74 | 0.05 | 1.65 | 1.82 |
| 360 | -1.97 | 0.05 | -2.06 | -1.88 |
| Distance | | | | |
| 1 | 10.21 | 0.14 | 9.98 | 10.44 |
| 2 | 8.45 | 0.14 | 8.22 | 8.68 |
| 3 | 4.46 | 0.14 | 4.23 | 4.69 |
| 4 | 3.73 | 0.14 | 3.50 | 3.96 |
| 5 | -0.88 | 0.14 | -1.11 | -0.65 |
| 6 | -2.04 | 0.14 | -2.27 | -1.81 |
| 7 | -0.82 | 0.14 | -1.05 | -0.59 |
| 8 | -0.26 | 0.14 | -0.49 | -0.03 |
| 9 | -0.28 | 0.14 | -0.51 | -0.05 |
| 10 | 0.16 | 0.14 | -0.07 | 0.39 |
| 11 | -0.52 | 0.14 | -0.75 | -0.29 |
| 12 | -0.95 | 0.14 | -1.18 | -0.72 |
| 13 | -1.11 | 0.14 | -1.34 | -0.88 |
| 14 | -1.61 | 0.14 | -1.84 | -1.38 |
| 15 | -1.81 | 0.14 | -2.03 | -1.58 |
| 16 | -2.28 | 0.14 | -2.51 | -2.05 |
| 17 | -2.66 | 0.14 | -2.88 | -2.43 |
| 18 | -2.40 | 0.14 | -2.63 | -2.17 |
| 19 | -2.83 | 0.14 | -3.06 | -2.60 |
| 20 | -3.28 | 0.14 | -3.50 | -3.05 |
| 21 | -3.29 | 0.14 | -3.52 | -3.06 |

* Not Significant

**Table 25. Computation of Effects for Experiment 3**

| | | Orientation | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | 90 | 180 | 270 | 360 | Row Sum | Row Mean | Row Effect |
| Distance | 1 | -0.14 | -11.82 | -1.31 | -5.14 | -18.41 | -4.60 | 8.23 |
| | 2 | -1.56 | -12.16 | -2.48 | -8.40 | -24.60 | -6.15 | 6.69 |
| | 3 | -5.21 | -15.00 | -8.94 | -10.79 | -39.94 | -9.99 | 2.85 |
| | 4 | -5.65 | -15.00 | -8.28 | -11.28 | -40.21 | -10.05 | 2.78 |
| | 5 | -11.10 | -15.00 | -14.34 | -14.50 | -54.94 | -13.74 | -0.90 |
| | 6 | -13.70 | -15.00 | -15.00 | -15.00 | -58.70 | -14.68 | -1.84 |
| | 7 | -11.98 | -15.00 | -13.42 | -15.00 | -55.40 | -13.85 | -1.01 |
| | 8 | -10.41 | -15.00 | -13.00 | -14.96 | -53.37 | -13.34 | -0.51 |
| | 9 | -9.83 | -15.00 | -13.00 | -14.66 | -52.49 | -13.12 | -0.29 |
| | 10 | -10.38 | -15.00 | -13.00 | -15.00 | -53.38 | -13.35 | -0.51 |
| | 11 | -11.06 | -15.00 | -13.00 | -15.00 | -54.06 | -13.52 | -0.68 |
| | 12 | -10.97 | -15.00 | -13.00 | -15.00 | -53.97 | -13.49 | -0.66 |
| | 13 | -12.14 | -15.00 | -13.00 | -15.00 | -55.14 | -13.79 | -0.95 |
| | 14 | -11.58 | -15.00 | -13.00 | -15.00 | -54.58 | -13.65 | -0.81 |
| | 15 | -12.58 | -15.00 | -14.00 | -15.00 | -56.58 | -14.15 | -1.31 |
| | 16 | -12.98 | -15.00 | -14.94 | -15.00 | -57.92 | -14.48 | -1.64 |
| | 17 | -13.00 | -15.00 | -15.00 | -15.00 | -58.00 | -14.50 | -1.66 |
| | 18 | -13.14 | -15.00 | -15.00 | -15.00 | -58.14 | -14.54 | -1.70 |
| | 19 | -13.46 | -15.00 | -15.00 | -15.00 | -58.46 | -14.62 | -1.78 |
| | 20 | -15.00 | -15.00 | -15.00 | -15.00 | -60.00 | -15.00 | -2.16 |
| | 21 | -15.00 | -15.00 | -15.00 | -15.00 | -60.00 | -15.00 | -2.16 |
| | Column Sum | -220.87 | -308.98 | -258.71 | -289.73 | -1078.29 | | |
| | Column Mean | -10.52 | -14.71 | -12.32 | -13.80 | | -12.84 | |
| | Column Effect | 2.32 | -1.88 | 0.52 | -0.96 | | | |

**Table 26. Error Computation for Experiment 3**

| | | Orientation | | | |
|---|---|---|---|---|---|
| | | 90 | 180 | 270 | 360 |
| Distance | 1 | 2.14 | -5.34 | 2.78 | 0.42 |
| | 2 | 2.27 | -4.13 | 3.15 | -1.29 |
| | 3 | 2.46 | -3.14 | 0.53 | 0.15 |
| | 4 | 2.08 | -3.07 | 1.26 | -0.27 |
| | 5 | 0.32 | 0.61 | -1.12 | 0.19 |
| | 6 | -1.34 | 1.55 | -0.84 | 0.63 |
| | 7 | -0.45 | 0.73 | -0.09 | -0.19 |
| | 8 | 0.61 | 0.22 | -0.17 | -0.66 |
| | 9 | 0.97 | 0.00 | -0.39 | -0.58 |
| | 10 | 0.65 | 0.22 | -0.17 | -0.70 |
| | 11 | 0.14 | 0.39 | 0.00 | -0.53 |
| | 12 | 0.20 | 0.37 | -0.02 | -0.55 |
| | 13 | -0.67 | 0.66 | 0.27 | -0.26 |
| | 14 | -0.25 | 0.52 | 0.13 | -0.40 |
| | 15 | -0.75 | 1.02 | -0.37 | 0.10 |
| | 16 | -0.82 | 1.36 | -0.98 | 0.44 |
| | 17 | -0.82 | 1.38 | -1.02 | 0.46 |
| | 18 | -0.92 | 1.41 | -0.98 | 0.49 |
| | 19 | -1.16 | 1.49 | -0.90 | 0.57 |
| | 20 | -2.32 | 1.88 | -0.52 | 0.96 |
| | 21 | -2.32 | 1.88 | -0.52 | 0.96 |

**Table 27. Error Squares for Experiment 3**

| | | Orientation | | | | |
|---|---|---|---|---|---|---|
| | | 90 | 180 | 270 | 360 | |
| Distance | 1 | 4.59 | 28.53 | 7.70 | 0.18 | 41.00 |
| | 2 | 5.16 | 17.09 | 9.94 | 1.66 | 33.85 |
| | 3 | 6.03 | 9.85 | 0.28 | 0.02 | 16.18 |
| | 4 | 4.34 | 9.43 | 1.58 | 0.07 | 15.42 |
| | 5 | 0.10 | 0.37 | 1.26 | 0.04 | 1.77 |
| | 6 | 1.81 | 2.41 | 0.71 | 0.40 | 5.33 |
| | 7 | 0.20 | 0.53 | 0.01 | 0.04 | 0.77 |
| | 8 | 0.38 | 0.05 | 0.03 | 0.43 | 0.89 |
| | 9 | 0.95 | 0.00 | 0.16 | 0.33 | 1.44 |
| | 10 | 0.42 | 0.05 | 0.03 | 0.48 | 0.98 |
| | 11 | 0.02 | 0.15 | 0.00 | 0.28 | 0.45 |
| | 12 | 0.04 | 0.14 | 0.00 | 0.30 | 0.48 |
| | 13 | 0.45 | 0.44 | 0.07 | 0.07 | 1.03 |
| | 14 | 0.06 | 0.27 | 0.02 | 0.16 | 0.51 |
| | 15 | 0.57 | 1.04 | 0.14 | 0.01 | 1.76 |
| | 16 | 0.67 | 1.84 | 0.96 | 0.19 | 3.66 |
| | 17 | 0.67 | 1.89 | 1.03 | 0.21 | 3.81 |
| | 18 | 0.85 | 1.99 | 0.96 | 0.24 | 4.06 |
| | 19 | 1.36 | 2.22 | 0.81 | 0.33 | 4.72 |
| | 20 | 5.38 | 3.52 | 0.27 | 0.92 | 10.09 |
| | 21 | 5.38 | 3.52 | 0.27 | 0.92 | 10.09 |

**Table 28. Sample Squares for Experiment 3**

| | | Orientation | | | | |
|---|---|---|---|---|---|---|
| | | 90 | 180 | 270 | 360 | Row Sum |
| Distance | 1 | 0.02 | 139.71 | 1.72 | 26.42 | 167.87 |
| | 2 | 2.43 | 147.87 | 6.15 | 70.56 | 227.01 |
| | 3 | 27.14 | 225.00 | 79.92 | 116.42 | 448.49 |
| | 4 | 31.92 | 225.00 | 68.56 | 127.24 | 452.72 |
| | 5 | 123.21 | 225.00 | 205.64 | 210.25 | 764.10 |
| | 6 | 187.69 | 225.00 | 225.00 | 225.00 | 862.69 |
| | 7 | 143.52 | 225.00 | 180.10 | 225.00 | 773.62 |
| | 8 | 108.37 | 225.00 | 169.00 | 223.80 | 726.17 |
| | 9 | 96.63 | 225.00 | 169.00 | 214.92 | 705.54 |
| | 10 | 107.74 | 225.00 | 169.00 | 225.00 | 726.74 |
| | 11 | 122.32 | 225.00 | 169.00 | 225.00 | 741.32 |
| | 12 | 120.34 | 225.00 | 169.00 | 225.00 | 739.34 |
| | 13 | 147.38 | 225.00 | 169.00 | 225.00 | 766.38 |
| | 14 | 134.10 | 225.00 | 169.00 | 225.00 | 753.10 |
| | 15 | 158.26 | 225.00 | 196.00 | 225.00 | 804.26 |
| | 16 | 168.48 | 225.00 | 223.20 | 225.00 | 841.68 |
| | 17 | 169.00 | 225.00 | 225.00 | 225.00 | 844.00 |
| | 18 | 172.66 | 225.00 | 225.00 | 225.00 | 847.66 |
| | 19 | 181.17 | 225.00 | 225.00 | 225.00 | 856.17 |
| | 20 | 225.00 | 225.00 | 225.00 | 225.00 | 900.00 |
| | 21 | 225.00 | 225.00 | 225.00 | 225.00 | 900.00 |
| | Column Sum | 2652.39 | 4562.58 | 3494.28 | 4139.61 | |

| | |
|---|---|
| SSY = | 14848.86 |
| SS0 = | 13841.78 |
| SSA = | 211.87 |
| SSB = | 633.38 |
| SSAB = | 158.28 |
| SST = | 1007.08 |
| SSE = | 3.56 |

| | |
|---|---|
| Explained by Orientation = | 21.04% |
| Explained by Distance = | 62.89% |
| Explained by Interactions = | 15.72% |
| Unexplained = | 0.35% |

**Table 29. ANOVA for Experiment 3**

| Component | Sum of Squares | Percentage of Variation | Degrees of Freedom | Mean Square | F-Computed | F-Table |
|---|---|---|---|---|---|---|
| y | 14848.86 | | 84 | | | |
| y.. | 13841.78 | | 1 | | | |
| y-y.. | 1007.08 | 100.00% | 83 | | | |
| Orientation | 211.87 | 21.04% | 3 | 70.62 | 1190.35 | 4.31 |
| Distance | 633.38 | 62.89% | 20 | 31.67 | 533.78 | 2.37 |
| Errors | 3.56 | 0.35% | 60 | 0.06 | | |

| | |
|---|---|
| Std Dev Errors = | 0.24 |
| Std Dev Mean = | 0.03 |
| Std Dev Orientation = | 0.05 |
| Std Dev Distance = | 0.12 |

**Table 30. 90% Confidence Intervals for Effects for Experiment 3**

| Parameter | Mean Effect | Std Dev | Conf Interval | |
|---|---|---|---|---|
| Mean | -12.84 | 0.03 | -12.88 | -12.79 |
| Orientation | | | | |
| 90 | 2.32 | 0.05 | 2.24 | 2.40 |
| 180 | -1.88 | 0.05 | -1.95 | -1.80 |
| 270 | 0.52 | 0.05 | 0.44 | 0.59 |
| 360 | -0.96 | 0.05 | -1.04 | -0.88 |
| Distance | | | | |
| 1 | 8.23 | 0.12 | 8.04 | 8.43 |
| 2 | 6.69 | 0.12 | 6.49 | 6.89 |
| 3 | 2.85 | 0.12 | 2.65 | 3.05 |
| 4 | 2.78 | 0.12 | 2.59 | 2.98 |
| 5 | -0.90 | 0.12 | -1.10 | -0.70 |
| 6 | -1.84 | 0.12 | -2.04 | -1.64 |
| 7 | -1.01 | 0.12 | -1.21 | -0.81 |
| 8 | -0.51 | 0.12 | -0.70 | -0.31 |
| 9 | -0.29 | 0.12 | -0.48 | -0.09 |
| 10 | -0.51 | 0.12 | -0.71 | -0.31 |
| 11 | -0.68 | 0.12 | -0.88 | -0.48 |
| 12 | -0.66 | 0.12 | -0.85 | -0.46 |
| 13 | -0.95 | 0.12 | -1.15 | -0.75 |
| 14 | -0.81 | 0.12 | -1.01 | -0.61 |
| 15 | -1.31 | 0.12 | -1.51 | -1.11 |
| 16 | -1.64 | 0.12 | -1.84 | -1.44 |
| 17 | -1.66 | 0.12 | -1.86 | -1.46 |
| 18 | -1.70 | 0.12 | -1.90 | -1.50 |
| 19 | -1.78 | 0.12 | -1.98 | -1.58 |
| 20 | -2.16 | 0.12 | -2.36 | -1.96 |
| 21 | -2.16 | 0.12 | -2.36 | -1.96 |

* Not Significant

**Table 31. Computation of Effects for Experiment 4**

| | | Orientation | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | 90 | 180 | 270 | 360 | Row Sum | Row Mean | Row Effect |
| Distance | 1 | 0.00 | -7.40 | 0.00 | -1.00 | -8.40 | -2.10 | 9.16 |
| | 2 | 0.00 | -10.02 | -0.14 | -5.00 | -15.16 | -3.79 | 7.47 |
| | 3 | -5.00 | -10.51 | -3.00 | -10.00 | -28.51 | -7.13 | 4.13 |
| | 4 | -3.00 | -11.24 | -5.00 | -10.00 | -29.24 | -7.31 | 3.95 |
| | 5 | -10.82 | -15.00 | -10.00 | -15.00 | -50.82 | -12.71 | -1.45 |
| | 6 | -15.00 | -15.00 | -13.00 | -15.00 | -58.00 | -14.50 | -3.24 |
| | 7 | -10.00 | -15.00 | -10.00 | -13.42 | -48.42 | -12.11 | -0.85 |
| | 8 | -10.00 | -13.00 | -6.06 | -15.00 | -44.06 | -11.02 | 0.24 |
| | 9 | -10.00 | -13.00 | -6.18 | -13.00 | -42.18 | -10.55 | 0.71 |
| | 10 | -10.00 | -13.00 | -7.88 | -13.00 | -43.88 | -10.97 | 0.29 |
| | 11 | -10.00 | -13.34 | -6.68 | -15.00 | -45.02 | -11.26 | 0.00 |
| | 12 | -10.00 | -13.00 | -9.82 | -15.00 | -47.82 | -11.96 | -0.70 |
| | 13 | -11.00 | -13.00 | -10.34 | -13.00 | -47.34 | -11.84 | -0.58 |
| | 14 | -11.00 | -13.88 | -13.00 | -15.00 | -52.88 | -13.22 | -1.96 |
| | 15 | -13.00 | -13.00 | -11.00 | -15.00 | -52.00 | -13.00 | -1.74 |
| | 16 | -12.54 | -14.54 | -11.00 | -15.00 | -53.08 | -13.27 | -2.01 |
| | 17 | -13.00 | -15.00 | -11.00 | -15.00 | -54.00 | -13.50 | -2.24 |
| | 18 | -13.00 | -15.00 | -11.80 | -15.00 | -54.80 | -13.70 | -2.44 |
| | 19 | -13.00 | -15.00 | -13.00 | -15.00 | -56.00 | -14.00 | -2.74 |
| | 20 | -13.00 | -15.00 | -13.00 | -15.00 | -56.00 | -14.00 | -2.74 |
| | 21 | -15.00 | -15.00 | -13.00 | -15.00 | -58.00 | -14.50 | -3.24 |
| | Column Sum | -208.36 | -278.93 | -184.90 | -273.42 | -945.61 | | |
| | Column Mean | -9.92 | -13.28 | -8.80 | -13.02 | | -11.26 | |
| | Column Effect | 1.34 | -2.03 | 2.45 | -1.76 | | | |

**Table 32. Error Computation for Experiment 4**

| | | Orientation | | | |
|---|---|---|---|---|---|
| | | 90 | 180 | 270 | 360 |
| Distance | 1 | 0.76 | -3.27 | -0.35 | 2.86 |
| | 2 | 2.45 | -4.20 | 1.20 | 0.55 |
| | 3 | 0.79 | -1.36 | 1.68 | -1.11 |
| | 4 | 2.97 | -1.90 | -0.14 | -0.93 |
| | 5 | 0.55 | -0.27 | 0.25 | -0.53 |
| | 6 | -1.84 | 1.53 | -0.95 | 1.26 |
| | 7 | 0.77 | -0.87 | -0.35 | 0.45 |
| | 8 | -0.32 | 0.04 | 2.50 | -2.22 |
| | 9 | -0.79 | -0.43 | 1.91 | -0.69 |
| | 10 | -0.37 | 0.00 | 0.64 | -0.27 |
| | 11 | -0.08 | -0.06 | 2.12 | -1.98 |
| | 12 | 0.62 | 0.98 | -0.32 | -1.28 |
| | 13 | -0.50 | 0.86 | -0.96 | 0.60 |
| | 14 | 0.88 | 1.37 | -2.23 | -0.02 |
| | 15 | -1.34 | 2.03 | -0.45 | -0.24 |
| | 16 | -0.61 | 0.76 | -0.18 | 0.03 |
| | 17 | -0.84 | 0.53 | 0.05 | 0.26 |
| | 18 | -0.64 | 0.73 | -0.55 | 0.46 |
| | 19 | -0.34 | 1.03 | -1.45 | 0.76 |
| | 20 | -0.34 | 1.03 | -1.45 | 0.76 |
| | 21 | -1.84 | 1.53 | -0.95 | 1.26 |

**Table 33. Error Squares for Experiment 4**

| | | Orientation | | | | |
|---|---|---|---|---|---|---|
| | | 90 | 180 | 270 | 360 | |
| Distance | 1 | 0.58 | 10.72 | 0.12 | 8.20 | 19.63 |
| | 2 | 6.03 | 17.68 | 1.43 | 0.31 | 25.45 |
| | 3 | 0.63 | 1.84 | 2.81 | 1.23 | 6.51 |
| | 4 | 8.85 | 3.63 | 0.02 | 0.86 | 13.36 |
| | 5 | 0.30 | 0.07 | 0.06 | 0.28 | 0.72 |
| | 6 | 3.37 | 2.33 | 0.91 | 1.59 | 8.20 |
| | 7 | 0.59 | 0.76 | 0.12 | 0.20 | 1.67 |
| | 8 | 0.10 | 0.00 | 6.26 | 4.94 | 11.31 |
| | 9 | 0.62 | 0.18 | 3.66 | 0.48 | 4.95 |
| | 10 | 0.13 | 0.00 | 0.41 | 0.07 | 0.61 |
| | 11 | 0.01 | 0.00 | 4.51 | 3.93 | 8.44 |
| | 12 | 0.38 | 0.96 | 0.10 | 1.64 | 3.09 |
| | 13 | 0.25 | 0.74 | 0.92 | 0.36 | 2.26 |
| | 14 | 0.78 | 1.86 | 4.98 | 0.00 | 7.63 |
| | 15 | 1.78 | 4.10 | 0.20 | 0.06 | 6.15 |
| | 16 | 0.37 | 0.57 | 0.03 | 0.00 | 0.97 |
| | 17 | 0.70 | 0.28 | 0.00 | 0.07 | 1.04 |
| | 18 | 0.40 | 0.53 | 0.31 | 0.21 | 1.45 |
| | 19 | 0.11 | 1.05 | 2.11 | 0.58 | 3.85 |
| | 20 | 0.11 | 1.05 | 2.11 | 0.58 | 3.85 |
| | 21 | 3.37 | 2.33 | 0.91 | 1.59 | 8.20 |

**Table 34. Sample Squares for Experiment 4**

| | | Orientation | | | | |
|---|---|---|---|---|---|---|
| | | 90 | 180 | 270 | 360 | Row Sum |
| Distance | 1 | 0.00 | 54.76 | 0.00 | 1.00 | 55.76 |
| | 2 | 0.00 | 100.40 | 0.02 | 25.00 | 125.42 |
| | 3 | 25.00 | 110.46 | 9.00 | 100.00 | 244.46 |
| | 4 | 9.00 | 126.34 | 25.00 | 100.00 | 260.34 |
| | 5 | 117.07 | 225.00 | 100.00 | 225.00 | 667.07 |
| | 6 | 225.00 | 225.00 | 169.00 | 225.00 | 844.00 |
| | 7 | 100.00 | 225.00 | 100.00 | 180.10 | 605.10 |
| | 8 | 100.00 | 169.00 | 36.72 | 225.00 | 530.72 |
| | 9 | 100.00 | 169.00 | 38.19 | 169.00 | 476.19 |
| | 10 | 100.00 | 169.00 | 62.09 | 169.00 | 500.09 |
| | 11 | 100.00 | 177.96 | 44.62 | 225.00 | 547.58 |
| | 12 | 100.00 | 169.00 | 96.43 | 225.00 | 590.43 |
| | 13 | 121.00 | 169.00 | 106.92 | 169.00 | 565.92 |
| | 14 | 121.00 | 192.65 | 169.00 | 225.00 | 707.65 |
| | 15 | 169.00 | 169.00 | 121.00 | 225.00 | 684.00 |
| | 16 | 157.25 | 211.41 | 121.00 | 225.00 | 714.66 |
| | 17 | 169.00 | 225.00 | 121.00 | 225.00 | 740.00 |
| | 18 | 169.00 | 225.00 | 139.24 | 225.00 | 758.24 |
| | 19 | 169.00 | 225.00 | 169.00 | 225.00 | 788.00 |
| | 20 | 169.00 | 225.00 | 169.00 | 225.00 | 788.00 |
| | 21 | 225.00 | 225.00 | 169.00 | 225.00 | 844.00 |
| Column Sum | | 2445.32 | 3787.98 | 1966.24 | 3838.10 | |

| | |
|---|---|
| SSY = | 12037.64 |
| SS0 = | 10644.98 |
| SSA = | 315.13 |
| SSB = | 936.25 |
| SSAB = | 139.34 |
| SST = | 1392.66 |
| SSE = | 1.95 |

| | |
|---|---|
| Explained by Orientation = | 22.63% |
| Explained by Distance = | 67.23% |
| Explained by Interactions = | 10.00% |
| Unexplained = | 0.14% |

**Table 35. ANOVA for Experiment 4**

| Component | Sum of Squares | Percentage of Variation | Degrees of Freedom | Mean Square | F-Computed | F-Table |
|---|---|---|---|---|---|---|
| y | 12037.64 | | 84 | | | |
| y.. | 10644.98 | | 1 | | | |
| y-y.. | 1392.66 | 100.00% | 83 | | | |
| Orientation | 315.13 | 22.63% | 3 | 105.04 | 3236.48 | 4.31 |
| Distance | 936.25 | 67.23% | 20 | 46.81 | 1442.32 | 2.37 |
| Errors | 1.95 | 0.14% | 60 | 0.03 | | |

| | |
|---|---|
| Std Dev Errors = | 0.18 |
| Std Dev Mean = | 0.02 |
| Std Dev Orientation = | 0.03 |
| Std Dev Distance = | 0.09 |

**Table 36. 90% Confidence Intervals for Effects for Experiment 4**

| Parameter | Mean Effect | Std Dev | Conf Interval | |
|---|---|---|---|---|
| Mean | -11.26 | 0.02 | -11.29 | -11.22 |
| Orientation | | | | |
| 90 | 1.34 | 0.03 | 1.28 | 1.39 |
| 180 | -2.03 | 0.03 | -2.08 | -1.97 |
| 270 | 2.45 | 0.03 | 2.40 | 2.51 |
| 360 | -1.76 | 0.03 | -1.82 | -1.71 |
| Distance | | | | |
| 1 | 9.16 | 0.09 | 9.01 | 9.30 |
| 2 | 7.47 | 0.09 | 7.32 | 7.61 |
| 3 | 4.13 | 0.09 | 3.98 | 4.28 |
| 4 | 3.95 | 0.09 | 3.80 | 4.09 |
| 5 | -1.45 | 0.09 | -1.59 | -1.30 |
| 6 | -3.24 | 0.09 | -3.39 | -3.10 |
| 7 | -0.85 | 0.09 | -0.99 | -0.70 |
| 8 | 0.24 | 0.09 | 0.10 | 0.39 |
| 9 | 0.71 | 0.09 | 0.57 | 0.86 |
| 10 | 0.29 | 0.09 | 0.14 | 0.43 |
| 11 | 0.00 | 0.09 | -0.14 | 0.15 |
| 12 | -0.70 | 0.09 | -0.84 | -0.55 |
| 13 | -0.58 | 0.09 | -0.72 | -0.43 |
| 14 | -1.96 | 0.09 | -2.11 | -1.82 |
| 15 | -1.74 | 0.09 | -1.89 | -1.60 |
| 16 | -2.01 | 0.09 | -2.16 | -1.87 |
| 17 | -2.24 | 0.09 | -2.39 | -2.10 |
| 18 | -2.44 | 0.09 | -2.59 | -2.30 |
| 19 | -2.74 | 0.09 | -2.89 | -2.60 |
| 20 | -2.74 | 0.09 | -2.89 | -2.60 |
| 21 | -3.24 | 0.09 | -3.39 | -3.10 |

* Not Significant

## *Bibliography*


[1] Angell, C., *Bluetooth as a 3G Enabler*, Marlow, UK, Entercai Mondiale Ltd, 2001

[2] Bisdikian, C., *An Overview of the Bluetooth Wireless Technology*, IEEE Communications Magazine, Dec 2001.

[3] Bluetooth SIG, *Bluetooth Capacity and Throughput*, SIG Forum, 2000.

[4] Bluetooth SIG, *Specification of the Bluetooth System Version 1.1*, **https://www.bluetooth.org**, 2001.

[5] CSR, *CSR's Implementation of HCI on BlueCore*, CSR, Cambridge, United Kingdom, 2001.

[6] Haas, J. and L. Zhou, *Securing Ad Hoc Networks*, Cornell University, IEEE Network, December, 1999.

[7] International Telecommunication Union, *Recommendation ITU-R M.1225, Guidelines for Evaluation of Radio Transmission Technologies for IMT-2000*, ITU, 1997.

[8] Jain, R., The Art of Computer Systems Performance Analysis, John Wiley & Sons, Inc., New York, 1991.

[9] Jakobsson, M. and S. Wetzel, *Security Weaknesses in Bluetooth*, Lucent Technologies and Bell Labs, Murray Hill, NJ, 2001.

[10] Kirk, M., *802.11*, SearchNetworking.com Definitions, **http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci341007,00.html**, 2002.

[11] Mettala, R., *Bluetooth Protocol Architecture*, *Version 1.0*, Bluetooth White Paper, Nokia Mobile Phones, 1999.

[12] Sheldon, T., Encyclopedia of Networking & Telecommunications, McGraw Hill, New York, 2001

[13] Singer, A., *802.15 aims to secure wireless PANs*, Network World Fusion, **http://www.nwfusion.com/news/tech/2002/0311tech.html**, 2002

[14] Symbol Technologies, *Bluetooth: The Leading Edge in Wireless Personal Area Networking*, Technology Brief, April 2001.

# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 074-0188*



| **1. REPORT DATE** *(DD-MM-YYYY)* | **2. REPORT TYPE** | **3. DATES COVERED** *(From – To)* |
|---|---|---|
| 25-03-2003 | Master's Thesis | Mar 2002 – Mar 2003 |

**4. TITLE AND SUBTITLE**

PERFORMANCE EVALUATION AND ANALYSIS OF EFFECTIVE RANGE AND DATA THROUGHPUT FOR UNMODIFIED BLUETOOTH COMMUNICATION DEVICES

**5a. CONTRACT NUMBER**

**5b. GRANT NUMBER**

**5c. PROGRAM ELEMENT NUMBER**

**6. AUTHOR(S)**

Kneeland, Timothy F., Captain, USAF

**5d. PROJECT NUMBER** ENG 02-252, 2002-048

**5e. TASK NUMBER**

**5f. WORK UNIT NUMBER**

**7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)**
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way, Building 640
Wright Patterson AFB OH 45433-7765

**8. PERFORMING ORGANIZATION REPORT NUMBER**

AFIT/GCS/ENG/03-08

**9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)**
Air Force Information Warfare Center/IODA
Attn: Mr. William Mueller — MAJCOM: ACC
404 Greig Street — Comm: 210-925-3588
San Antonio, TX 78226 — e-mail: william.mueller@lackland.af.mil

**10. SPONSOR/MONITOR'S ACRONYM(S)**

AFIWC

**11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

**12. DISTRIBUTION/AVAILABILITY STATEMENT**

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

**13. SUPPLEMENTARY NOTES**

**14. ABSTRACT**

The DoD and the Air Force continually seek to incorporate new technology in an effort to improve communication, work effectiveness, and efficiency. Office devices utilizing Bluetooth technology simplify device configuration and communication. They provide a means to communicate wirelessly over short distances thereby eliminating the need for different vendor specific cables and interfaces. One of the key concerns involved in incorporating new communication technology is security; the fundamental security concern of wireless communication is interception. Studies focusing on IEEE 802.11b have shown vulnerability zones around many DoD installations that reflect the ranges at which wireless communications using the 802.11b standard can be intercepted.

This research identifies the vulnerability zones in which Bluetooth transmissions can potentially be intercepted. Specifically, the orientation of Bluetooth device antenna and the distance between devices are varied to determine ranges at which set levels of throughput can be achieved for a specific device configuration. Throughput ranges are then mapped to graphically reflect vulnerability zones. This research shows that the range at which Bluetooth communication can occur with unmodified devices is more than twice that of the minimum standard of 10m outlined in the core specification without degradation of the best-case throughput level measured. It is expected that the throughput ranges could be greatly extended with some device modification. This research shows that the security risk associated with interception of Bluetooth communications is legitimate and warrants further study.

**15. SUBJECT TERMS**

Ad hoc networks, Antenna radiation patterns, Bluetooth, Communications networks, Computer networks, Computer communications, Data links, Data rate, Data transmissions systems, Networks, Personal area networks, Rates, Telecommunications, Throughput, Wireless communications

| **16. SECURITY CLASSIFICATION OF:** | | | **17. LIMITATION OF ABSTRACT** | **18. NUMBER OF PAGES** | **19a. NAME OF RESPONSIBLE PERSON** |
|---|---|---|---|---|---|
| **a. REPORT** | **b. ABSTRACT** | **c. THIS PAGE** | | | Dr. Richard A. Raines |
| **U** | **U** | **U** | **UU** | 108 | **19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-6565, ext 4278; e-mail: richard.raines@afit.edu |